Asynchronous Transfer Mode Configuration Guide, Cisco IOS Release 15M&T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 22

CHAPTER 1

Configuring ATM

This chapter describes how to configure ATM on Cisco routers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

How to Configure ATM

To configure ATM, complete the tasks in the following sections. The first task is required, and then you must configure at least one PVC or SVC. The virtual circuit options you configure must match in three places: on the router, on the ATM switch, and at the remote end of the PVC or SVC connection. The remaining tasks are optional.

Enabling Configuring the ATM Interface

This section describes how to configure an ATM interface. For the Advanced Inspection and Prevention Security Services (AIP), all ATM port adapters, and the 1-port ATM-25 network module, the port number is always 0. For example, the *slot*/*port* address of an ATM interface on an AIP installed in slot 1 is 1/0.

Perform the following task to enable the ATM interface:

SUMMARY STEPS

1. **configure terminal**
2. Do one of the following:
    - **interface atm** *slot* **/0**
    - **interface atm** *slot* **/** *port-adapter* **/0**
3. **ip address** *ip-address mask*
4. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode from the terminal.
Step 2	Do one of the following: • **interface atm** *slot* **/0** • **interface atm** *slot* **/** *port-adapter* **/0** **Example:** `Router(config)#` **interface atm** *number*	Specifies the ATM interface using the appropriate format of the **interface atm** command. To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.
Step 3	**ip address** *ip-address mask*	(Optional) If IP routing is enabled on the system, assigns a source IP address and subnet mask to the interface.
Step 4	**no shutdown**	Changes the shutdown state to up and enables the ATM interface, thereby beginning the segmentation and reassembly (SAR) operation on the interface. • The **no shutdown** command passes an **enable** command to the ATM interface, which then begins segmentation and reassembly (SAR) operations. It also causes the ATM interface to configure itself based on the previous configuration commands sent.

Configuring PVCs

To use a permanent virtual circuit (PVC), you must configure the PVC into both the router and the ATM switch. PVCs remain active until the circuit is removed from either configuration.

Note If you use PVC discovery, you do not have to configure the PVC on the router. Refer to the section "Configuring PVC Discovery, on page 5" for more information.

When a PVC is configured, all the configuration options are passed on to the ATM interface. These PVCs are writable into the nonvolatile RAM (NVRAM) as part of the Route Processor (RP) configuration and are used when the RP image is reloaded.

Some ATM switches might have point-to-multipoint PVCs that do the equivalent task of broadcasting. If a point-to-multipoint PVC exists, then that PVC can be used as the sole broadcast PVC for all multicast requests.

To configure a PVC, perform the tasks in the following sections. The first two tasks are required; the other tasks are optional.

Creating a PVC

Note After configuring the parameters for an ATM PVC, you must exit interface-ATM-VC configuration mode in order to create the PVC and enable the settings.

To create a PVC on the ATM interface and enter interface-ATM-VC configuration mode, use the following command beginning in interface configuration mode:

Command	Purpose
`Router(config-if)#` **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers. Enters interface-ATM-VC configuration mode. Optionally configures ILMI, QSAAL, or SMDS encapsulation. • Once you specify a name for a PVC, you can reenter the interface-ATM-VC configuration mode by simply entering **pvc** *name*. • The **ilmi** keyword in the **pvc** command is used for setting up an ILMI PVC in an SVC environment. Refer to the section "Configuring Communication with the ILMI" later in this chapter for more information. • See examples of PVC configurations in the section "ATM Configuration Examples, on page 103" at the end of this chapter.

Mapping a Protocol Address to a PVC

The ATM interface supports a static mapping scheme that identifies the network address of remote hosts or routers. This section describes how to map a PVC to an address, which is a required task for configuring a PVC.

Note If you enable or disable broadcasting directly on a PVC using the **protocol** command, this configuration will take precedence over any direct configuration using the **broadcast** command.

See examples of PVC configurations in the section "ATM Configuration Examples, on page 103" at the end of this chapter.

To map a protocol address to a PVC, use the following command in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)#` **protocol** *protocol* *protocol-address* `[[`**no**`]` **broadcast**`]`	Maps a protocol address to a PVC.

Configuring the AAL and Encapsulation Type

To configure the ATM adaptation layer (AAL) and encapsulation type, use the following command beginning in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)#` **encapsulation aal5** *encap*	Configures the ATM adaptation layer (AAL) and encapsulation type. • 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 Asynchronous Transfer Mode Command Reference*. The global default is AAL5 with SNAP encapsulation.

Configuring PVC Traffic Parameters

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

Note The commands in this section are not supported on the ATM port adapter (PA-A1 series). The ABR service class is only supported on the ATM-CES port adapter for PVCs. The 1-port ATM-25 network module only supports UBR.

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

For an example of how to configure an ABR PVC, refer to the section "Example Configuring an ABR PVC, on page 105" at the end of this chapter.

For a description of how to configure traffic parameters in a VC class and apply the VC class to an ATM interface or subinterface, refer to the section "Configuring VC Classes, on page 28."

To configure PVC traffic parameters, use one of the following commands beginning in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)#` **abr** *output-pcr output-mcr*	Configures the Available Bit Rate (ABR). (ATM-CES port adapter and Multiport T1/E1 ATM Network Module only.)
`Router(config-if-atm-vc)#` **ubr** *output-pcr*	Configures the Unspecified Bit Rate (UBR).
`Router(config-if-atm-vc)#` **ubr+** *output-pcr output-mcr*	Configures the UBR and a minimum guaranteed rate.
`Router(config-if-atm-vc)#` **vbr-nrt** *output-pcr output-scr output-mbs*	Configures the Variable Bit Rate-Non Real Time (VBR-NRT) QOS.
`Router(config-if-atm-vc)#` **vbr-rt** *peak-rate average-rate burst*	Configures the real-time Variable Bit Rate (VBR). (Cisco MC3810 and Multiport T1/E1 ATM Network Module only.)

Configuring ABR VCs

For ABR VCs, you can optionally configure the amount that the cell transmission rate increases or decreases in response to flow control information from the network or destination. For an example of configuring an ABR PVC, see the section "Example Configuring an ABR PVC, on page 105" later in this chapter.

To configure this option, use the following command in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)#` **atm abr rate-factor** [*rate-increase-factor*] [*rate-decrease-factor*]	Specifies the ABR rate factors. The default increase and decrease rate factors is 1/16.

Configuring PVC Discovery

You can configure your router to automatically discover PVCs that are configured on an attached adjacent switch. The discovered PVCs and their traffic parameters are configured on an ATM main interface or subinterface that you specify. Your router receives the PVC parameter information using Interim Local Management Interface (ILMI). For an example of configuring PVC discovery, refer to the section "Example Configuring PVC Discovery, on page 105" at the end of this chapter.

To configure PVC discovery on an ATM interface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**
2. Router(config-if)# **pvc** [*name*] **0/16 ilmi**
3. Router(config-if-atm-vc)# **exit**
4. Router(config-if)# **atm ilmi-pvc-discovery** [**subinterface**]
5. Router(config-if)# **exit**
6. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
7. Router(config-subif)# **ip address** *ip-address mask*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0** • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0** **Example:** **Example:**	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]

	Command or Action	Purpose
	Example: `Router(config)#` **interface atm** *number*	
Step 2	Router(config-if)# **pvc** [*name*] **0/16 ilmi**	Configures an ILMI PVC on the main interface.
Step 3	Router(config-if-atm-vc)# **exit**	Returns to interface configuration mode.
Step 4	Router(config-if)# **atm ilmi-pvc-discovery** [**subinterface**]	Configures PVC Discovery on the main interface and optionally specifies that discovered PVCs will be assigned to a subinterface.
Step 5	Router(config-if)# **exit**	Returns to global configuration mode.
Step 6	Do one of the following: • Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** `Router(config)#` **interface atm** *number*`[`**.** *subinterface-number* `{`**multipoint** `|` **point-to-point**`}]`	Specifies the ATM main interface or subinterface that discovered PVCs will be assigned to. • Use the **subinterface** keyword in Step 4 if you want the discovered PVCs to reside on an ATM subinterface that you specify in Step 6. The discovered PVCs are assigned to the subinterface number that matches the VPI number of the discovered PVC. For example, if subinterface 2/0.1 is specified using the **interface atm** command in Step 6, then all discovered PVCs with a VPI value of 1 will be assigned to this subinterface. For an example, see the section "Example Configuring PVC Discovery, on page 105" later in this chapter. • Repeat Steps 6 and 7 if you want discovered PVCs to be assigned to more than one subinterface. If no subinterfaces are configured, discovered PVCs will be assigned to the main interface specified in Step 1.
Step 7	Router(config-subif)# **ip address** *ip-address mask*	(Optional) Specifies the protocol address for the subinterface.

1 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Enabling Inverse ARP

Inverse ARP is enabled by default when you create a PVC using the **pvc** command. Once configured, a protocol mapping between an ATM PVC and a network address is learned dynamically as a result of the exchange of ATM Inverse ARP packets.

Inverse ARP is supported on PVCs running IP or IPX and no static map is configured. If a static map is configured, Inverse ARP will be disabled.

When PVC discovery is enabled on an active PVC and the router terminates that PVC, the PVC will generate an ATM Inverse ARP request. This allows the PVC to resolve its own network addresses without configuring a static map.

Address mappings learned through Inverse ARP are aged out. However, mappings are refreshed periodically. This period is configurable using the **inarp** command, which has a default of 15 minutes.

You can also enable Inverse ARP using the **protocol** command. This is necessary only if you disabled Inverse ARP using the **no protocol** command. For more information about this command, refer to the "ATM Commands" chapter in the *Cisco IOS Asynchronous Transfer Mode Command Reference*.

For an example of configuring Inverse ARP, see the section "Example Enabling Inverse ARP, on page 106" at the end of this chapter.

To enable Inverse ARP on an ATM PVC, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
    - Router(config)# **interface atm** *slot* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}]
    -
    -
    - Router(config)# **interface atm** *slot* / *port-adapter* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}]
2. **pvc** [*name*] *vpi* / *vci*
3. **encapsulation aal5snap**
4. **inarp** *minutes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}] • •	Specifies the ATM interface using the appropriate format of the **interface atm** command.[2]

	Command or Action	Purpose
	• Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)#` **interface atm** *number*[**.** *subinterface-number* {**multipoint** | **point-to-point**}]	
Step 2	**pvc** [*name*] *vpi* / *vci*	Specifies an ATM PVC by name (optional) and VPI/VCI numbers.
Step 3	**encapsulation aal5snap**	Configures AAL5 LLC-SNAP encapsulation if it is not already configured.
Step 4	**inarp** *minutes*	(Optional) Adjusts the Inverse ARP time period.

2 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring Loopback Cells to Verify Connectivity

You can optionally configure the PVC to generate end-to-end F5 OAM loopback cells to verify connectivity on the virtual circuit. The remote end must respond by echoing back such cells. If OAM response cells are missed (indicating the lack of connectivity), the PVC state goes down. If all the PVCs on a subinterface go down, the subinterface goes down.

For information about managing PVCs using OAM, see the section "Configuring OAM Management for PVCs and SVCs, on page 34" later in this chapter.

For an example of OAM loopback cell generation, see the section "Example Configuring Loopback Cells, on page 106" at the end of this chapter.

To configure transmission of end-to-end F5 OAM cells on a PVC, use the following commands in interface-ATM-VC configuration mode:

SUMMARY STEPS

1. Router(config-if-atm-vc)# **oam-pvc** [**manage**] *frequency*
2. Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if-atm-vc)# **oam-pvc** [**manage**] *frequency*	Configures transmission of end-to-end F5 OAM loopback cells on a PVC, specifies how often loopback cells should be sent, and optionally enables OAM management of the connection.
Step 2	Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is only supported if OAM management is enabled. • Use the *up-count*argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a PVC connection state to up. Use the *down-count* argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to tear down a PVC. Use the *retry-frequency* argument to specify the frequency (in seconds) that end-to-end F5 OAM loopback cells should be transmitted when a change in UP/DOWN state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *frequency* (in seconds) specified using the **oam-pvc** command, then loopback cells are sent at the *retry-frequency* to verify whether or not the PVC is down.

Configuring Broadcast on a PVC

To send duplicate broadcast packets for all protocols configured on a PVC, use the following command in interface-ATM-VC configuration mode:

Note If you enable or disable broadcasting directly on a PVC using the **protocol** command, this configuration will take precedence over any direct configuration using the **broadcast** command.

Command	Purpose
`Router(config-if-atm-vc)#` **broadcast**	Sends duplicate broadcast packets for all protocols configured on a PVC.

Assigning a VC Class to a PVC

By creating a VC class, you can preconfigure a set of default parameters that you may apply to a PVC. To create a VC class, refer to the section "Configuring VC Classes, on page 28" later in this chapter.

Once you have created a VC class, use the following command in interface-ATM-VC configuration mode to apply the VC class to a PVC:

Command	Purpose
`Router(config-if-atm-vc)#` **class-vc** *vc-class-name*	Applies a VC class to a PVC. • The *vc-class-name* argument is the same as the *name* argument you specified when you created a VC class using the **vc-class atm** command. Refer to the section "Configuring VC Classes, on page 28" later in this chapter for a description of how to create a VC class.

Configuring PVC Trap Support

You can configure the PVC to provide failure notification by sending a trap when a PVC on an ATM interface fails or leaves the UP operational state.

PVC Failure Notification

Only one trap is generated per hardware interface, within the specified interval defined by the interval "atmIntPvcNotificationInterval". If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the interval has elapsed. Once the interval has elapsed, the traps are sent if the PVCs are still DOWN.

No trap is generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router.

PVC Status Tables

When PVC trap support is enabled, the SNMP manager can poll the SNMP agent to get PCV status information. The table "atmInterfaceExtTable" provides PVC status on an ATM interface. The table "atmCurrentlyFailingPVclTable" provides currently failing and previously failed PVC time-stamp information.

Note PVC traps are only supported on permanent virtual circuit links (PVCLs), and not on permanent virtual path links (PVPLs).

Prerequisites

Before you enable PVC trap support, you must configure SNMP support and an IP routing protocol on your router. See the "ATM Configuration Examples, on page 103" section later in this document. For more information about configuring SNMP support, refer to the chapter "Configuring SNMP Support" in the Cisco IOS Configuration Fundamentals Configuration Guide . For information about configuring IP routing protocols, refer to the section "IP Routing Protocols" in the Cisco IOS IP Configuration Guide .

To receive PVC failure notification and access to PVC status tables on your router, you must have the Cisco PVC trap MIB called CISCO-IETF-ATM2-PVCTRAP-MIB.my compiled in your NMS application. You can find this MIB on the Web at Cisco's MIB website that has the URL http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Enabling PVC Trap Support

When you configure PVC trap support, you must also enable OAM management on the PVC.

For more information on OAM management, see the section "Configuring OAM Management for PVCs and SVCs, on page 34" later in this chapter.

The new objects in this feature are defined in the IETF draft The Definitions of Supplemental Managed Objects for ATM Management , which is an extension to the AToM MIB (RFC 1695).

For an example of configuring PVC trap support, see the section "Example Configuring PVC Trap Support, on page 106" at the end of this chapter.

To enable PVC trap support and OAM management, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **snmp-server enable traps atm pvc interval** *seconds* **fail-interval** *seconds*
2. Do one of the following:
    - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
    -
    -
    - Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
3. Router(config-if)# **pvc**[*name*] *vpi* / *vci*
4. Router(config-if-atm-vc)# **oam-pvc manage**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **snmp-server enable traps atm pvc interval** *seconds* **fail-interval** *seconds*	Enables PVC trap support.
Step 2	Do one of the following: • Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]	Specifies the ATM interface using the appropriate form of the **interface atm** command.[3]

	Command or Action	Purpose
	Example: **Example:** **Example:** `Router(config)#` **interface atm** *number*`[`**.** *subinterface-number* `{`**multipoint | point-to-point**`}]`	
Step 3	Router(config-if)# **pvc**[*name*] *vpi* / *vci*	Enables the PVC.
Step 4	Router(config-if-atm-vc)# **oam-pvc manage**	Enables end-to-end OAM management for an ATM PVC.

3 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring SVCs

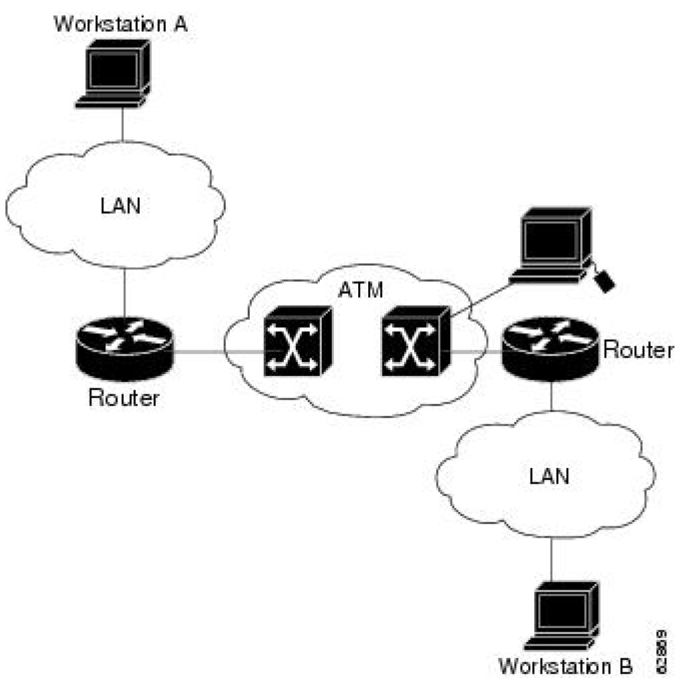
ATM switched virtual circuit (SVC) service operates much like X.25 SVC service, although ATM allows much higher throughput. Virtual circuits are created and released dynamically, providing user bandwidth on demand. This service requires a signaling protocol between the router and the switch.

The ATM signaling software provides a method of dynamically establishing, maintaining, and clearing ATM connections at the User-Network Interface (UNI). The ATM signaling software conforms to ATM Forum UNI 3.0 or ATM Forum UNI 3.1 depending on what version is selected by ILMI or configuration.

In UNI mode, the user is the router and the network is an ATM switch. This is an important distinction. The Cisco router does not perform ATM-level call routing. Instead, the ATM switch does 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.

The figure below illustrates the router position in a basic ATM environment. The router is used primarily to interconnect LANs via an ATM network. The workstation connected directly to the destination ATM switch illustrates that you can connect not only routers to ATM switches, but also any computer with an ATM interface that conforms to the ATM Forum UNI specification.

Figure 1: Basic ATM Environment



Some of the tasks in the following sections are optional SVC tasks for customizing your network. These tasks are considered advanced; the default values are almost always adequate. You need not perform these tasks unless you need to customize your particular SVC connection.

Note SVCs are not supported on the 1-port ATM-25 network module.

Configuring Communication with the ILMI

In an SVC environment, you must configure a PVC for communication with the Integrated Local Management Interface (ILMI) so that 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.

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

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.

For an example of configuring ILMI, see the section "Example Configuring Communication with the ILMI, on page 107" in the "ATM Configuration Examples, on page 103" section at the end of this chapter.

To configure ILMI communication and optionally enable the ILMI keep alive funciton, use the following command in interface configuration mode:

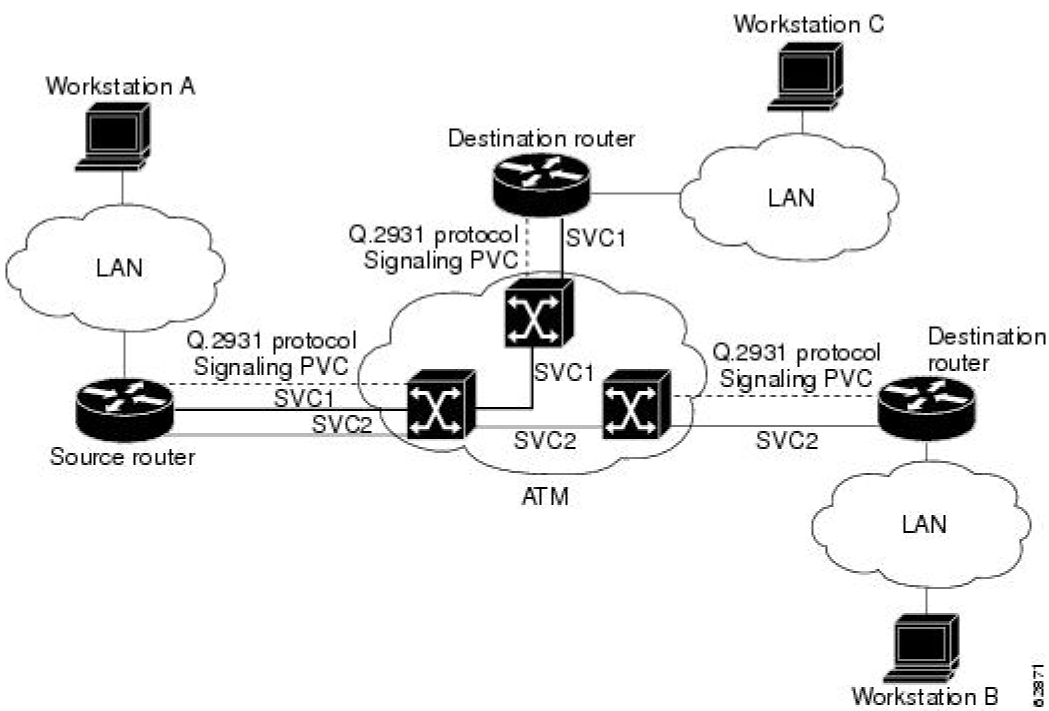
Command	Purpose
Router(config-if)# **pvc** [*name*] **0/16 ilmi**	Creates an ILMI PVC on an ATM main interface.
Router(config-if)# **atm ilmi-keepalive** [*seconds*]	(Optional) Enables ILMI keepalives and sets the interval between keepalives.

Configuring the PVC That Performs SVC Call Setup

Unlike X.25 service, which uses in-band signaling (connection establishment done on the same circuit as data transfer), ATM uses out-of-band signaling. 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. The signaling that accomplishes the call setup and teardown is called *Layer 3 signaling* or the *Q.2931 protocol* .

For out-of-band signaling, a signaling PVC must be configured before any SVCs can be set up. The figure below illustrates that a signaling PVC from the source router to the ATM switch is used to set up two SVCs. This is a fully meshed network; workstations A, B, and C all can communicate with each other.

Figure 2: One or More SVCs Require a Signaling PVC



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 local switch. The standard value for VPI and VCI are 0 and 5, respectively.

See the section "Example SVCs in a Fully Meshed Network, on page 107" at the end of this chapter for a sample ATM signaling configuration.

To configure the signaling PVC for all SVC connections, use the following command in interface configuration mode:

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

Configuring the NSAP Address

Every 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.

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 via ILMI, you can configure the endstation 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.

The recommended *vpi* and *vci* values for the ILMI PVC are 0 and 16, respectively.

You can also specify a keepalive interval for the ILMI PVC. See the "Configuring Communication with the ILMI, on page 14" section earlier in this chapter for more information.

To see an example of setting up the ILMI PVC and assigning the ESI and selector fields of an NSAP address, see the section "Example SVCs with Multipoint Signaling, on page 108" at the end of this chapter.

To configure the router to get the NSAP prefix from the switch and use locally entered values for the remaining fields of the address, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **pvc** [*name*] **0/16 ilmi**
2. Router(config-if-atm-vc)# **exit**
3. Router(config-if)# **atm esi-address** *esi* **.** *selector*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **pvc** [*name*] **0/16 ilmi**	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.

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 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.

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. For information about using the **atm esi-address** command, see the preceding section "Configuring the ESI and Selector Fields, on page 16."

See an example of assigning an NSAP address to an ATM interface in the section "Example ATM NSAP Address, on page 108" at the end of this chapter.

Because the interface has no default NSAP address, you must configure the NSAP address for SVCs. To set the ATM interface's source NSAP address, use the following command in interface configuration mode:

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

Creating an SVC

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

To create an SVC, use the following commands beginning in interface configuration mode.

Note Cisco IOS software does not support creation of SVCs on a point-to-point subinterface.

SUMMARY STEPS

1. Router(config-if)# **svc** [*name*] **nsap** *address*
2. Router(config-if-atm-vc)# **encapsulation aal5** *encap*
3. Router(config-if-atm-vc)# **protocol** *protocol protocol-address* [[**no**] **broadcast**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **svc** [*name*] **nsap** *address*	Creates an SVC and specifies the destination NSAP address.
Step 2	Router(config-if-atm-vc)# **encapsulation aal5** *encap*	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. • For a list of AAL types and encapsulations supported for the *aal-encap* argument, refer to the **encapsulation aal5**command in the *Cisco IOS Asynchronous Transfer Mode Command Reference*. The default is AAL5 with SNAP encapsulation.
Step 3	Router(config-if-atm-vc)# **protocol** *protocol protocol-address* [[**no**] **broadcast**]	Maps a protocol address to an SVC.

Configuring ATM UNI Version Override

Normally, when ILMI link autodetermination is enabled on the interface and is successful, the router takes the user-network interface (UNI) version returned by ILMI. If the ILMI link autodetermination process is unsuccessful or ILMI is disabled, the UNI version defaults to 3.0. You can override this default by using the **atm uni-version** command. The **no** form of the command sets the UNI version to the one returned by ILMI if ILMI is enabled and the link autodetermination is successful. Otherwise, the UNI version will revert to 3.0. To override the ATM UNI version used by the router, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm uni-version** *version-number*	Overrides UNI version used by router.

Configuring the Idle Timeout Interval

You can specify an interval of inactivity after which any idle SVC on an interface is torn down. This timeout interval might help control costs and free router memory and other resources for other uses.

In addition to configuring the interval of inactivity, you can optionally specify the minimum-ratein kilobits per second (kbps). This is the minimum traffic rate required on an ATM SVC to maintain the connection.

To change the idle timeout interval, use the following command in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)#` **idle-timeout** *seconds* [*minimum-rate*]	Configures the interval of inactivity after which an idle SVC will be torn down.

Configuring Point-to-Multipoint Signaling

Point-to-multipoint signaling (or multicasting) allows the router to send one packet to the ATM switch and have the switch replicate the packet to the destinations. It replaces pseudobroadcasting on specified virtual circuits for protocols configured for broadcasting.

You can configure multipoint signaling on an ATM interface after you have mapped protocol addresses to NSAPs and configured one or more protocols for broadcasting.

After multipoint signaling is set, the router uses the SVC configurations that have the **broadcast** keyword set to establish multipoint calls. The call is established to the first destination with a Setup message. Additional parties are added to the call with AddParty messages each time a multicast packet is sent. One multipoint call will be established for each logical subnet of each protocol that has the **broadcast** keyword set.

If multipoint virtual circuits are closed, they are reopened with the next multicast packet. Once the call is established, additional parties are added to the call when additional multicast packets are sent. If a destination never comes up, the router constantly attempts to add it to the call by means of multipoint signaling.

For an example of configuring multipoint signaling on an interface that is configured for SVCs, see the section "Example SVCs with Multipoint Signaling, on page 108" at the end of this chapter.

To configure multipoint signaling on an ATM interface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**
2. Router(config-if)# **pvc** [*name*] **0/5 qsaal**
3. Router(config-if-atm-vc)# **exit**
4. Router(config-if-atm-vc)# **pvc** [*name*] **0/16 ilmi**
5. Do one of the following:
   - Router(config-if)# **atm nsap-address** *nsap-address*
   -
   -
   - Router(config-if)# **atm esi-address** *esi* **.** *selector*
6. Router(config-if)# **svc** [*name*] **nsap** *address*
7. Router(config-if-atm-vc)# **protocol** *protocol protocol-address* **broadcast**
8. Router(config-if-atm-vc)# **exit**
9. Router(config-if)# **atm multipoint-signalling**
10. Router(config-if)# **atm multipoint-interval interval**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0** • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0** **Example:** **Example:**	Specifies the ATM interface using the appropriate format of the **interface atm** command.[4]

	Command or Action	Purpose
	Example: `Router(config)#` **interface atm** *number*	
Step 2	Router(config-if)# **pvc** [*name*] **0/5 qsaal**	Configures the signaling PVC for an ATM main interface that uses SVCs.
Step 3	Router(config-if-atm-vc)# **exit**	Returns to interface configuration mode.
Step 4	Router(config-if-atm-vc)# **pvc** [*name*] **0/16 ilmi** **Example:** **Example:** `and` **Example:** `Router(config-if-atm-vc)#` **exit**	(Optional) Configures an ILMI PVC on an ATM main interface and returns to interface configuration mode. This task is required if you configure the ATM NSAP address in Step 5 by configuring the ESI and selector fields.
Step 5	Do one of the following: • Router(config-if)# **atm nsap-address** *nsap-address* • • • Router(config-if)# **atm esi-address** *esi* **.** *selector*	Configures the complete NSAP address manually. or Configures the ESI and selector fields. To use this method, you must configure Step 4 first.
Step 6	Router(config-if)# **svc** [*name*] **nsap** *address*	Create san SVC and specifies the destination NSAP address. Enters interface-ATM-VC mode.
Step 7	Router(config-if-atm-vc)# **protocol** *protocol protocol-address* **broadcast**	Provides a protocol address for the interface and enables broadcasting.
Step 8	Router(config-if-atm-vc)# **exit**	Returns to interface configuration mode.
Step 9	Router(config-if)# **atm multipoint-signalling**	Enables multipoint signaling to the ATM switch.
Step 10	Router(config-if)# **atm multipoint-interval interval**	(Optional) Limits the frequency of sending AddParty messages.

4 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring IP Multicast over ATM Point-to-Multipoint Virtual Circuits

This task is documented in the "Configuring IP Multicast Routing" chapter of the Cisco IOS IP Configuration Guide .

Configuring SVC Traffic Parameters

The tasks in this section are optional and advanced. The ATM signaling software can specify to the ATM interface on the router and the switch a limit on how much traffic the source router will be sending. It provides this information in the form of traffic parameters. (These parameters have default values.) The ATM switch in turn sends these values as requested by the source to the ATM destination node. If the destination cannot provide such capacity levels, the call may fail. (For Cisco router series behavior, see the per-interface **atm sig-traffic-shaping strict** command in the *Cisco IOS Wide-Area Networking Command Reference*.) There is a single attempt to match traffic values.

The supported traffic parameters are part of the following service categories: Unspecified bit rate (UBR), UBR+, and variable bit rate nonreal-time (VBR-NRT). Only one of these categories can be specified per SVC connection so if a new one is entered, it will replace the existing one. The commands used to specify the service category and traffic values are identical to those used when you create a PVC.

Note The commands in this section are not supported on the ATM port adapter (PA-A1 series). The 1-port ATM-25 network module only supports UBR.

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

For an example of configuring traffic parameters on an SVC, see the section "Example Configuring SVC Traffic Parameters, on page 109" at the end of this chapter.

For a description of how to configure traffic parameters in a VC class and apply the VC class to an ATM interface or subinterface, refer to the section "Configuring VC Classes, on page 28."

To configure traffic parameters on an SVC, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
2. Router(config-if)# **svc** [*name*] **nsap** *address*
3. Router(config-if-atm-vc)# **protocol** *protocol protocol-address* [[**no**] **broadcast**]
4. Do one of the following:
   - Router(config-if-atm-vc)# **ubr** *output-pcr* [*input-pcr*]
   -
   -
   - Router(config-if-atm-vc)# **ubr+** *output-pcr output-mcr* [*input-pcr*] [*input-mcr*]
5. Router(config-if-atm-vc)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** `Router(config)#` **interface atm** *number*`[`**.** *subinterface-number* `{`**multipoint** `|` **point-to-point**`}]`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[5]

	Command or Action	Purpose
Step 2	Router(config-if)# **svc** [*name*] **nsap** *address*	Creates an SVC and specifies the destination NSAP address.
Step 3	Router(config-if-atm-vc)# **protocol** *protocol protocol-address* [[**no**] **broadcast**]	Maps a destination protocol address to an SVC.
Step 4	Do one of the following: • Router(config-if-atm-vc)# **ubr** *output-pcr* [*input-pcr*] • • • Router(config-if-atm-vc)# **ubr+** *output-pcr output-mcr* [*input-pcr*] [*input-mcr*] **Example:** **Example:** **Example:** Router(config-if-atm-vc)# **vbr-nrt** *output-pcr output-scr output-mbs* [*input-pcr*] [*input-scr*] [*input-mbs*]	Configures the UBR or Configures the UBR and a minimum guaranteed rate or Configures the VBR-NRT QOS.
Step 5	Router(config-if-atm-vc)# **exit**	Returns to interface configuration mode and enables the traffic parameters on the SVC.

5 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring Strict Traffic Shaping

You can configure strict traffic shaping on an ATM interface to specify that an SVC be established using only signaled traffic parameters. If such shaping cannot be provided, the SVC is released.

If you do not configure strict traffic shaping on the router ATM interface, an attempt is made to establish an SVC with traffic shaping for the transmit cell flow per the signaled traffic parameters. If such shaping cannot be provided, the SVC is installed with default shaping parameters; that is, it behaves as though a PVC were created without specifying traffic parameters.

To specify that an SVC be established on an ATM interface using only signaled traffic parameters, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm sig-traffic-shaping strict**	Specifies that an SVC be established on an ATM interface using only signaled traffic parameters.

Configuring Loopback Cells to Verify SVC Connectivity

You can optionally configure the SVC to generate end-to-end F5 OAM loopback cells to verify connectivity on the virtual circuit. The remote end must respond by echoing back such cells. If OAM response cells are missed (indicating the lack of connectivity), the SVC is torn down. For more information, refer to the "Configuring OAM Management for PVCs and SVCs, on page 34" section later in this chapter.

Note Generally, ATM signaling manages ATM SVCs. Configuring the **oam-svc** command on an SVC verifies the inband integrity of the SVC.

To configure transmission of end-to-end F5 OAM loopback cells on an SVC, use the following commands in interface-ATM-VC configuration mode:

SUMMARY STEPS

1. Router(config-if-atm-vc)# **oam-svc** [**manage**] *frequency*
2. Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if-atm-vc)# **oam-svc** [**manage**] *frequency*	Configures transmission of end-to-end F5 OAM loopback cells on an SVC, specifies how often loopback cells should be sent, and optionally enables OAM management of the connection.
Step 2	Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of an SVC connection. This command is only supported if OAM management is enabled. • The *up-count*argument does not apply to SVCs, but it must be specified in order to configure the *down-count* and *retry-frequency*. Use the *down-count* argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to tear down an SVC. Use the *retry-frequency* argument to specify the frequency (in seconds) that end-to-end F5 OAM loopback cells should be transmitted when a change in UP/DOWN state is being verified. For example, if an SVC is up and a loopback cell response is not received after the *frequency* (in seconds) specified using the **oam-svc** command, then loopback cells are sent at the *retry-frequency* to verify whether or not the SVC is down.

Configuring Broadcast on an SVC

To send duplicate broadcast packets or send a single broadcast packet using multipoint signaling for all protocols configured on an SVC, use the following command in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)#` **broadcast**	Sends duplicate broadcast packets for all protocols configured on an SVC. • If you enable or disable broadcasting directly on an SVC using the **protocol** command, this configuration will take precedence over any direct configuration using the **broadcast** command.

Assigning a VC Class to an SVC

By creating a VC class, you can preconfigure a set of default parameters that you may apply to an SVC. To create a VC class, refer to the section "Configuring VC Classes, on page 28" later in this chapter.

Once you have created a VC class, use the following command in interface-ATM-VC configuration mode to apply the VC class to an SVC:

Command	Purpose
`Router(config-if-atm-vc)#` **class-vc** *vc-class-name*	Applies a VC class to an SVC. • The *vc-class-name* argument is the same as the *name* argument you specified when you created a VC class using the **vc-class atm** command. Refer to the section "Configuring VC Classes, on page 28" later in this chapter for a description of how to create a VC class.

Configuring SSCOP

The Service-Specific Connection-Oriented Protocol (SSCOP) resides in the service-specific convergence sublayer (SSCS) of the ATM adaptation layer (AAL). SSCOP is used to transfer variable-length service data units (SDUs) between users of SSCOP. SSCOP provides for the recovery of lost or corrupted SDUs.

Note The tasks in this section customize the SSCOP feature to a particular network or environment and are optional. The features have default values and are valid in most installations. Before customizing these features, you should have a good understanding of SSCOP and the network involved.

Setting the Poll Timer

The poll timer controls the maximum time between transmission of a POLL PDU when sequential data (SD) or SDP PDUs are queued for transmission or are outstanding pending acknowledgments. To change the poll timer from the default value of 100 seconds, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **sscop poll-timer** *seconds*	Sets the poll timer.

Setting the Keepalive Timer

The keepalive timer controls the maximum time between transmission of a POLL PDU when no SD or SDP PDUs are queued for transmission or are outstanding pending acknowledgments. To change the keepalive timer from the default value of 5 seconds, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if-atm-vc)#` **sscop keepalive-timer** *seconds*	Sets the keepalive timer.

Setting the Connection Control Timer

The connection control timer determines the time between transmission of BGN, END, or RS (resynchronization) PDUs as long as an acknowledgment has not been received. Connection control performs the establishment, release, and resynchronization of an SSCOP connection.

To change the connection control timer from the default value of 1 seconds and to optionally change the retry count of the connection control timer from the default value of 10, use the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)#` **sscop cc-timer** *seconds*	Sets the connection control timer.
`Router(config-if)#` **sscop max-cc** *retries*	(Optional) Sets the number of times that SSCOP will retry to transmit BGN, END, or RS PDUs when they have not been acknowledged.

Setting the Transmitter and Receiver Windows

A transmitter window controls how many packets can be transmitted before an acknowledgment is required. A receiver window controls how many packets can be received before an acknowledgment is required.

To change the transmitter's window from the default value of 7 and to change the receiver's window from the default value of 7, use the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)#` **sscop send-window** *packets*	Sets the transmitter's window.
`Router(config-if)#` **sscop receive-window** *packets*	Sets the receiver's window.

Closing an SVC

You can disconnect an idle SVC by using the following command in EXEC mode:

Command	Purpose
`Router #` **atmsig close atm** *slot* **/0** *vcd*	(Optional) Closes the signaling PVC for an SVC.

Configuring VC Classes

A VC class is a set of preconfigured VC parameters that you configure and apply to a particular VC or ATM interface. You may apply a VC class to an ATM main interface, subinterface, PVC, or SVC. For example, you can create a VC class that contains VC parameter configurations that you will apply to a particular PVC or SVC. You might create another VC class that contains VC parameter configurations that you will apply to all VCs configured on a particular ATM main interface or subinterface. Refer to the "ATM Configuration Examples, on page 103" section later in this chapter for examples of VC class configurations.

Creating a VC Class

To create a VC class, use the following command in global configuration mode:

For examples of creating VC classes, see the section "Example Creating a VC Class, on page 109" at the end of this chapter.

Command	Purpose
`Router(config)#` **vc-class atm** *name*	Creates a VC class and enters vc-class configuration mode.

Configuring VC Parameters

After you create a VC class and enter vc-class configuration mode, configure VC parameters using one or more of the following commands:

- **abr**
- **broadcast**
- **encapsulation aal5**
- **idle-timeout**
- **ilmi manage**
- **inarp**
- **oam-pvc**
- **oam retry**
- **oam-svc**
- **protocol**
- **ubr**
- **ubr+**
- **vbr-nrt**

Refer to the sections "Configuring PVCs, on page 2" and "Configuring PVC Trap Support, on page 11" for descriptions of how to configure these commands for PVCs and SVCs.

If an SVC command (for example, **idle-timeout** or **oam-svc**) is configured in a VC class, but the VC class is applied on a PVC, the SVC command is ignored. This is also true if a PVC command is applied to an SVC.

For examples of creating VC classes, see the section "Example Creating a VC Class, on page 109" at the end of this chapter.

Applying a VC Class on an ATM PVC or SVC

Once you have created and configured a VC class, you can apply it directly on an ATM PVC or SVC, or you can apply it on an ATM interface or subinterface.

To apply a VC class directly on an ATM PVC or SVC, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Do one of the following:
    - Router(config-if)# **pvc** [*name*] *vpi* / *vci*
    -
    -
    - Router(config-if)# **svc** [*name*] **nsap** *address*
2. Router(config-if-atm-vc)# **class-vc** *vc-class-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config-if)# **pvc** [*name*] *vpi* / *vci* • • • Router(config-if)# **svc** [*name*] **nsap** *address*	Specifies an ATM PVC. or Specifies an ATM SVC.
Step 2	Router(config-if-atm-vc)# **class-vc** *vc-class-name*	Applies a VC class directly on the PVC or SVC.

Applying a VC Class on an ATM Interface

To apply a VC class on an ATM main interface or subinterface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
    - Router(config)# **interface atm** *slot* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
    -
    -
    - Router(config)# **interface atm** *slot* / *port-adapter* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
2. Router(config-if)# **class-int** *vc-class-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** `Router(config)#` **interface atm** *number*`[`**.** *subinterface-number* `{`**multipoint** `|` **point-to-point**`}]`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[6]
Step 2	Router(config-if)# **class-int** *vc-class-name*	Applies a VC class on an the ATM main interface or subinterface.

6 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring VC Management

When you configure VC management, you enable the router to detect VC connections and disconnections automatically. This notifies protocols to reroute packets immediately, preventing protocols from waiting for unpredictable and relatively long timeout periods.

You may use Integrated Local Management Interface (ILMI) or operation, administration, and maintenance (OAM) or both for managing your PVCs, and OAM for managing your SVCs. For PVCs, you must decide which method is reliable in your particular network.

When ILMI and OAM management methods are both configured to manage a PVC, both must indicate that a PVC is up in order for that PVC to be determined as up. If either ILMI or OAM is not configured, a PVC will be managed by the method that is configured.

When a PVC goes down, route caches for protocols configured on that PVC are cleared (or flushed) so that new routes may be learned. The route cache flush is applied on the PVC's interface. When all PVCs on a subinterface go down, VC management shuts down the subinterface, in addition to flushing route caches.

ATM hardware must keep the PVC active, however, so that OAM and ILMI cells may flow. When any PVC on a subinterface comes up, the subinterface is brought up.

VC management using ILMI is referred to as ILMI management. VC management using OAM is referred to as OAM management. To configure either management method or both, perform the tasks in one or both of the following sections:

Configuring ILMI Management

The PVC comes up only if ILMI indicates the PVC is up. The PVC comes down when ILMI indicates that the PVC is down. If OAM management is also configured for the same PVC, the PVC comes up only if both ILMI and OAM indicate that the PVC is up.

For an example of configuring ILMI management on a PVC, see the section "Example LMI Management on an ATM PVC, on page 110" at the end of this chapter.

ILMI management applies to PVCs only. To configure ILMI management, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* /**0**[**.** *subinterface-number*{**multipoint** | **point-to-point**}]
2. Router(config-if)# **pvc** [*name*] **0/16 ilmi**
3. Do one of the following:
   - Router(config)# **interface atm** *slot* /**0.** *subinterface-number* **multipoint**
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* /**0.** *subinterface-number* **multipoint**
4. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
5. Router(config-if-atm-vc)# **ilmi manage**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] •	Specifies the ATM interface using the appropriate format of the **interface atm** command.[7]

	Command or Action	Purpose
	• • Router(config)# **interface atm** *slot* / *port-adapter* **/0[.** *subinterface-number*{**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** Router(config)# **interface atm** *number*[**.** *subinterface-number* {**multipoint** | **point-to-point**}]	
Step 2	Router(config-if)# **pvc** [*name*] **0/16 ilmi**	Configures a PVC for communication with the ILMI.
Step 3	Do one of the following: • Router(config)# **interface atm** *slot* **/0.** *subinterface-number* **multipoint** • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0.** *subinterface-number* **multipoint** **Example:** **Example:** **Example:** Router(config)# **interface atm** *number* **.** *subinterface-number* **multipoint**	(Optional) Specifies the ATM subinterface of the PVC you want to manage.
Step 4	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Specifies the PVC to be managed.
Step 5	Router(config-if-atm-vc)# **ilmi manage**	Enables ILMI management on the PVC. • Repeat Steps 4 and 5 for each PVC you want to manage. Step 3 is necessary only if you want to configure a PVC on a subinterface and not just on the main ATM interface.

	Command or Action	Purpose

7 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring OAM Management for PVCs and SVCs

OAM management may be enabled for both PVCs and SVCs. To configure OAM management, perform the tasks in one or both of the following sections:

Configuring OAM Management for PVCs

By default, end-to-end F5 OAM loopback cell generation is turned off for each PVC. A PVC is determined as down when any of the following is true on that PVC:

- The router does not receive a loopback reply after a configured number of retries of sending end-to-end F5 OAM loopback cells.
- The router receives a Virtual Circuit-Alarm Indication Signals (VC-AIS) cell.
- The router receives a Virtual Circuit-Remote Detect Indicator (VC-RDI) cell.

A PVC is determined as up when all of the following are true on that PVC:

- The router receives a configured number of successive end-to-end F5 OAM loopback cell replies.
- The router does not receive VC-AIS cell for 3 seconds.
- The router does not receive VC-RDI cell for 3 seconds.

For an example of configuring OAM management on a PVC, see the section "Example OAM Management on an ATM SVC, on page 111" at the end of this chapter.

To configure OAM management for an ATM PVC, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint | point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint | point-to-point**}]
2. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
3. Router(config-if-atm-vc)# **oam-pvc manage** [*frequency*]
4. Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** `Router(config)# Router(config)#` **interface atm** *number*[**.** *subinterface-number* {**multipoint** | **point-to-point**}]	Specifies the ATM interface using the appropriate format of the **interface atm** command.[8]
Step 2	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Specifies the ATM PVC.
Step 3	Router(config-if-atm-vc)# **oam-pvc manage** [*frequency*]	Enables OAM management on the PVC.
Step 4	Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for reestablishing and removing a PVC connection. • Use the *up-count* argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a PVC connection state to up. Use the *down-count* argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to tear down a PVC. Use the *retry-frequency* argument to specify the frequency (in seconds) that end-to-end F5 OAM loopback cells should be transmitted when a change in UP/DOWN state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *frequency* (in seconds) specified using the **oam-pvc** command, then loopback cells are sent at the *retry-frequency* to verify whether or not the PVC is down.

	Command or Action	Purpose

8 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring OAM Management for SVCs

If OAM management is enabled on SVCs and detects disconnection on an SVC, that SVC is torn down.

For an example of configuring OAM management on an SVC, see the section "Example OAM Management on an ATM SVC, on page 111" at the end of this chapter.

To configure OAM management for an ATM SVC, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
2. Router(config-if)# **svc** [*name*] **nsap** *address*
3. Router(config-if-atm-vc)# **oam-svc manage** [*frequency*]
4. Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:**	Specifies the ATM interface using the appropriate format of the **interface atm** command.[9]

	Command or Action	Purpose
	Example: **Example:** `Router(config)#` **interface atm** *number*`[`**.** *subinterface-number* `{`**multipoint** `|` **point-to-point**`}]`	
Step 2	Router(config-if)# **svc** [*name*] **nsap** *address*	Specifies the ATM SVC.
Step 3	Router(config-if-atm-vc)# **oam-svc manage** [*frequency*]	Enables OAM management on the SVC.
Step 4	Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for re-establishing and removing an SVC connection. • The *up-count*argument does not apply to SVCs, but it must be specified in order to configure the *down-count* and *retry-frequency*. Use the *down-count* argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to tear down an SVC. Use the *retry-frequency* argument to specify the frequency (in seconds) at which end-to-end F5 OAM loopback cells should be transmitted when a change in UP/DOWN state is being verified. For example, if an SVC is up and a loopback cell response is not received after the *frequency* (in seconds) specified using the **oam-svc** command, then loopback cells are sent at the *retry-frequency* to verify whether or not the SVC is down.

[9] To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring Classical IP and ARP over ATM

Cisco implements both the ATM Address Resolution Protocol (ARP) server and ATM ARP client functions described in RFC 1577. RFC 1577 models an ATM network as a logical IP subnetwork on a LAN.

The tasks required to configure classical IP and ARP over ATM depend on whether the environment uses SVCs or PVCs.

Configuring Classical IP and ARP in an SVC Environment

The ATM ARP mechanism is applicable to networks that use SVCs. It requires a network administrator to configure only the device’s own ATM address and that of a single ATM ARP server into each client device.

When the client makes a connection to the ATM ARP server, the server sends ATM Inverse ARP requests to learn the IP network address and ATM address of the client on the network. It uses the addresses to resolve future ATM ARP requests from clients. Static configuration of the server is not required or needed.

In Cisco's implementation, the ATM ARP client tries to maintain a connection to the ATM ARP server. The ATM ARP server can tear down the connection, but the client attempts once each minute to bring the connection back up. No error messages are generated for a failed connection, but the client will not route packets until the ATM ARP server is connected and translates IP network addresses.

For each packet with an unknown IP address, the client sends an ATM ARP request to the server. Until that address is resolved, any IP packet routed to the ATM interface will cause the client to send another ATM ARP request. When the ARP server responds, the client opens a connection to the new destination so that any additional packets can be routed to it.

Cisco routers may be configured as ATM ARP clients to work with any ATM ARP server conforming to RFC 1577. Alternatively, one of the Cisco routers in a logical IP subnet (LIS) may be configured to act as the ATM ARP server itself. In this case, it automatically acts as a client as well. To configure classical IP and ARP in an SVC environment, perform the tasks in one of the following sections:

Configuring the Router as an ATM ARP Client

For an example of configuring the ATM ARP client, see the section "Example Configuring ATM ARP Client in an SVC Environment, on page 111" at the end of this chapter.

In an SVC environment, configure the ATM ARP mechanism on the interface by using the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**
2. Router(config-if)# **atm esi-address** *esi* **.** *selector*
3. Router(config-if)# **ip address** *address mask*
4. Router(config-if)# **atm classic-ip-extensions BFI**
5. Router(config-if)# **atm arp-server nsap** *nsap-address*
6. Router(config-if)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0** •	Specifies the ATM interface using the appropriate format of the **interface atm** command.[10]

	Command or Action	Purpose
	• • Router(config)# **interface atm** *slot* / *port-adapter* /**0** **Example:** **Example:** **Example:** `Router(config)#` **interface atm** *number*	
Step 2	Router(config-if)# **atm esi-address** *esi* **.** *selector*	Specifies the ATM address of the interface. • To configure the ESI and selector fields, the switch must be capable of delivering the NSAP address prefix to the router via ILMI and the router must be configured with a PVC for communication with the switch via ILMI. For a description of how to configure an ILMI PVC, refer to the section "Configuring Communication with the ILMI, on page 14" earlier in this chapter.
Step 3	Router(config-if)# **ip address** *address mask*	Specifies the IP address of the interface.
Step 4	Router(config-if)# **atm classic-ip-extensions BFI**	(Optional) Enables redundant ATM ARP servers. • You can designate the current router interface as the ATM ARP server by typing **self** in place of **nsap** *nsap-address*.
Step 5	Router(config-if)# **atm arp-server nsap** *nsap-address*	Specifies the ATM address of the ATM ARP server. Enter this command twice to specify two ATM ARP servers.
Step 6	Router(config-if)# **no shutdown**	Enables the ATM interface.

10 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring the Router as an ATM ARP Server

Cisco's implementation of the ATM ARP server supports redundant ATM ARP servers on a single logical IP subnetwork (LIS). In order for redundant ATM ARP server support to work, all of the devices on the LIS must be Cisco devices and must have the **atm classic-ip-extensions BFI** command configured. For an example of configuring the ATM ARP server, see the section "Example Configuring ATM ARP Client in an SVC Environment, on page 111" at the end of this chapter.

To configure the ATM ARP server, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* /**0**
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* /**0**
2. Router(config-if)# **atm esi-address** *esi* **.** *selector*
3. Router(config-if)# **ip address** *address mask*
4. Router(config-if)# **atm classic-ip-extensions BFI**
5. Router(config-if)# **atm arp-server self**
6. Router(config-if)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* /**0** • • • Router(config)# **interface atm** *slot* / *port-adapter* /**0** **Example:** **Example:** **Example:** `Router(config)#` **interface atm** *number*	Specifies the ATM interface using the appropriate format of the **interface atm** command.[11]
Step 2	Router(config-if)# **atm esi-address** *esi* **.** *selector*	Specifies the ATM address of the interface. • To configure the ESI and selector fields, the switch must be capable of delivering the NSAP address prefix to the router via ILMI and the router must be configured with a PVC for communication with the switch via ILMI. For a description of how to configure an ILMI PVC, refer to the section

	Command or Action	Purpose
		"Configuring Communication with the ILMI, on page 14" earlier in this chapter.
Step 3	Router(config-if)# **ip address** *address mask*	Specifies the IP address of the interface.
Step 4	Router(config-if)# **atm classic-ip-extensions BFI**	(Optional) Enables redundant ATM ARP servers.
Step 5	Router(config-if)# **atm arp-server self**	Identifies the ATM ARP server for the IP subnetwork network.
Step 6	Router(config-if)# **no shutdown**	Enables the ATM interface.

11 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring Classical IP and Inverse ARP in a PVC Environment

The ATM Inverse ARP mechanism is applicable to networks that use PVCs, where connections are established, but the network addresses of the remote ends are not known. A server function is not used in this mode of operation.

By default, Inverse ARP datagrams will be sent on this virtual circuit every 15 minutes. To adjust the Inverse ARP time period, use the **inarp** *minutes* command in interface-ATM-VC configuration mode.

Note The ATM ARP mechanism works with IP only. The Inverse ATM ARP mechanism works with IP and IPX only. For all other protocols, the destination address must be specified.

In a PVC environment, the ATM Inverse ARP mechanism is enabled by default for IP and IPX when you use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**
   -
   -
   - Router(config)# **interface atm** *slot* **/** *port-adapter* **/0**
2. Router(config-if)# **ip address** *address mask*
3. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
4. Router(config-if-atm-vc)# **no shutdown**
5.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* /**0** • • • Router(config)# **interface atm** *slot* / *port-adapter* /**0** **Example:** **Example:** **Example:** `Router(config)#` **interface atm** *number*	Specifies the ATM interface using the appropriate format of the **interface atm** command.[12]
Step 2	Router(config-if)# **ip address** *address mask*	Specifies the IP address of the interface.
Step 3	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Creates a PVC.
Step 4	Router(config-if-atm-vc)# **no shutdown**	Enables the ATM interface.
Step 5		Repeat Step 3 for each PVC you want to create.

12 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Customizing the ATM Interface

You can customize the ATM interface. The features you can customize have default values that will most likely suit your environment and probably need not be changed. However, you might need to enter configuration commands, depending upon the requirements for your system configuration and the protocols you plan to route on the interface. To customize the ATM interface, perform the tasks in the following sections:

Configuring the Rate Queue

A rate queue defines the speed at which individual virtual circuits will transmit data to the remote end. You can configure permanent rate queues, allow the software to set up dynamic rate queues, or perform some combination of the two. The software dynamically creates rate queues when you create a VC with a peak rate that does not match any user-configured rate queue. The software dynamically creates all rate queues if you have not configured any.

> **Note** You can only configure the rate queue for the AIP and NPM.

Using Dynamic Rate Queues

The Cisco IOS software automatically creates rate queues as necessary when you create a VC. If you do not configure traffic shaping on a VC, the peak rate of the VC is set to the UBR at the maximum peak rate that the physical layer interface module (PLIM) will allow. A rate queue is then dynamically created for the peak rate of that VC.

If dynamic rate queues do not satisfy your traffic shaping needs, you can configure permanent rate queues. Refer to the section "Configuring a Permanent Rate Queue, on page 44" for more information.

See the section "Examples Dynamic Rate Queue, on page 112" for example configurations of different rate queues.

Configuring Rate Queue Tolerance

To improve rate queue usage, you can configure a peak cell rate tolerance range for dynamically created rate queues. A PVC or SVC requesting a particular rate queue speed will be assigned to a rate queue that is within the range of the peak cell rate tolerance. If no such rate queue exists, a new rate queue is dynamically created on the ATM interface.

To configure a rate queue tolerance range for VCs on an ATM interface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
    - Router(config)# **interface atm** *slot* **/0**
    -
    -
    - Router(config)# **interface atm** *slot* / *port-adapter* **/0**
2. Router(config-if)# **atm rate-queue tolerance svc** [**pvc**] *tolerance-value* [**strict**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0** • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0**	Specifies the ATM interface using the appropriate format of the **interface atm** command.[13]

	Command or Action	Purpose
	Example: **Example:** **Example:** `Router(config)#` **interface atm** *number*	
Step 2	Router(config-if)# **atm rate-queue tolerance svc** [**pvc**] *tolerance-value* [**strict**]	Configures a rate queue tolerance. • The value for the *tolerance-value* argumentis expressed as a percentage used for assigning rate queues for each VC with a requested peak rate. This value is applied to SVCs, discovered VCs, and PVCs (when the **pvc** keyword is used). This value can be 0 or 5 through 99. For SVCs and discovered VCs, the default value is 10. If the pvc keyword is not specified, the rate queue tolerance for PVCs will default to 0.

13 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring a Permanent Rate Queue

The supports up to eight different peak rates. The peak rate is the maximum rate, in kilobits per second, at which a virtual circuit can transmit. Once attached to this rate queue, the virtual circuit is assumed to have its peak rate set to that of the rate queue. The rate queues are broken into a high-priority (0 through 3) and low-priority (4 through 7) bank.

You can configure each permanent rate queue independently to a portion of the overall bandwidth available on the ATM link. The combined bandwidths of all rate queues should not exceed the total bandwidth available. The total bandwidth depends on the PLIM (see the "ATM Interface Types" section in the "Wide-Area Networking Overview" chapter.)

To set a permanent rate queue, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm rate-queue** *queue-number speed*	Configures a permanent rate queue, which defines the maximum speed at which an individual virtual circuit transmits data to a remote ATM host.

Configuring MTU Size

Each interface has a default maximum packet size or maximum transmission unit (MTU) size. For ATM interfaces, this number defaults to 4470 bytes. The maximum is 9188 bytes for the AIP and NPM, 17969 for the ATM port adapter, and 17998 for the ATM-CES port adapter. The MTU can be set on a per-sub-interface basis as long as the interface MTU is as large or larger than the largest subinterface MTU.

For ATM interfaces, the MTU displays the following behavior:

- A new subinterface inherits the MTU from the main interface.
- The MTU is inherited from the main interface when there is a default setting on the subinterface MTU.
- A user configured MTU is nv-gened, even if the MTU is the same as/default MTU or the sub MTU of the main interface.
- If you have not explicitly specified the MTU, after a reload, by default, the subinterface MTU inherits the main interface.
- A change in the main interface MTU does not trigger a change in the subinterface MTUs. However, subsequently created subinterfaces inherit the same main interface MTU.

To set the maximum MTU size, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **mtu** *bytes*	Sets the maximum MTU size.

Setting the SONET PLIM

The default SONET PLIM is STS-3C. The default for DS3 is C-Bit ADM framing; the default for E3 is G.751 with PLCP framing.

To set the SONET PLIM to STM-1 or to set the PLIM framing for E3 or DS3, use one of the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm sonet stm-1**	Sets the OC-3c SONET PLIM to STM-1.
`Router(config-if)#` **atm framing** [**cbitadm** | **cbitplcp** | **m23adm** | **m23plcp**]	Sets DS3 framing mode.
`Router(config-if)#` **atm framing** [**g751adm** | **g832 adm** | **g751plcp**]	Sets E3 framing mode.

Setting Loopback Mode

Use these commands to set the loopback mode:

Command	Purpose
`Router(config-if)#` **loopback**	Sets loopback mode. Loops all packets back to your ATM interface instead of the network.
`Router(config-if)#` **loopback line**	Sets line loopback mode. Loops the incoming network packets back to the ATM network.

Setting the Exception Queue Length

The exception queue is used for reporting ATM events, such as CRC errors.

Note This command is supported only on the AIP.

By default, it holds 32 entries; the range is 8 to 256. It is unlikely that you will need to configure the exception queue length; if you do, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm exception-queue** *number*	Sets the exception queue length.

Configuring the Maximum Number of Channels

The **atm max-channels** command, available if you are using the ATM-CES port adapter, can be used to divide the available number (fixed) of transmit descriptors across the configured number of transmit channels. Typically, you think of a one-to-one association between a transmit channel and a VC; however, the ATM-CES port adapter supports types of VCs other than data VCs (for example CES VCs). Also, the ATM-CES port adapter can multiplex one or more VCs over a single virtual path (VP) that is shaped, and the VP only requires a single transmit channel. Therefore, the term transmit channel is used rather than virtual circuit.

The maximum burst of packets that are allowed per VC is limited by the number of transmit descriptors allocated per VC. Because the total number of transmit descriptors available is limited by the available SRAM space, configuration of the number of transmit channels for the interface determines the number of transmit descriptors for each transmit channel. Hence, the burst size for each transmit channel is determined by the **atm max-channels** command. For example, for 64 (default) numbers of transmit channels for the interface, 255 transmit descriptors are associated per transmit channel and for 512 numbers of transmit channels for the interface, 31 transmit descriptors are associated per transmit channel.

Note This command is available only on the ATM-CES port adapter.

To configure the maximum number of transmit channels for the interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm max-channels** *number*	Configures the maximum number of transmit channels.

Limiting the Number of Virtual Circuits

By default, the ATM interface allows the maximum of 2048 virtual circuits. However, you can configure a lower number, thereby limiting the number of virtual circuits on which your ATM interface allows segmentation and reassembly to occur. Limiting the number of virtual circuits does not affect the VPI-VCI pair of each virtual circuit.

Note This command is not supported on the ATM-CES port adapter or the NPM.

To set the maximum number of virtual circuits supported (including PVCs and SVCs), use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm maxvc** *number*	Limits the number of virtual circuits.

Setting the Raw-Queue Size

The raw queue is used for raw ATM cells, which include operation, administration, and maintenance (OAM) and Interim Local Management Interface (ILMI) cells. ILMI is a means of passing information to the router, including information about virtual connections and addresses. The raw-queue size is in the range of 8 to 256 cells; the default is 32 cells.

Note This command is supported only on the AIP.

To set the raw-queue size, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm rawq-size** *number*	Sets the raw-queue size.

Configuring Buffer Size

The number of receive buffers determines the maximum number of reassemblies that your ATM interface can perform simultaneously. The number of buffers defaults to 256, although it can be in the range from 0 to 512.

The number of transmit buffers determines the maximum number of fragmentations that your ATM interface can perform simultaneously. The number of buffers defaults to 256, although it can be in the range from 0 to 512.

Note The commands in this section are not supported on the ATM-CES port adapter or NPM.

To set the number of receive and transmit buffers, use the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm rxbuff** *number*	Sets the number of receive buffers.
`Router(config-if)#` **atm txbuff** *number*	Sets the number of transmit buffers.

Setting the VCI-to-VPI Ratio

By default, the ATM interface supports 1024 VCIs per VPI. Depending on what ATM interface card or port adapter you are using, this value can be any power of 2 in the range of 16 to 8192. (See the **atm vc-per-vp** command in the *Cisco IOS Wide-Area Networking Command Reference* for the exact values that apply to your configuration.) This value controls the memory allocation on your ATM interface that deals with the VCI table. It defines only the maximum number of VCIs to support per VPI.

To set the maximum number of VCIs to support per VPI and limit the highest VCI accordingly, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm vc-per-vp** *number*	Sets the number of VCIs per VPI.

Setting the Source of the Transmit Clock

By default, your ATM interface expects the ATM switch to provide transmit clocking. To specify that the ATM interface generates the transmit clock internally for SONET and E3 PLIM operation, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm clock internal**	Specifies that the ATM interface generates the transmit clock internally.

Configuring ATM Subinterfaces for SMDS Networks

An ATM adaptation layer (AAL) defines the conversion of user information into cells by segmenting upper-layer information into cells at the transmitter and reassembling them at the receiver. AAL1 and AAL2 handle isochronous traffic, such as voice and video, and are not relevant to the router. AAL3/4 and AAL5 support data communications by segmenting and reassembling packets. Beginning in Cisco IOS Release 10.2, we support both AAL3/4 and AAL5.

Our implementation of the AAL3/4 encapsulates each AAL3/4 packet in a Switched Multimegabit Data Service (SMDS) header and trailer. This feature supports both unicast and multicast addressing, and provides subinterfaces for multiple AAL3/4 connections over the same physical interface.

Note Each subinterface configured to support AAL3/4 is allowed only one SMDS E.164 unicast address and one E.164 multicast address. The multicast address is used for all broadcast operations. In addition, only one virtual circuit is allowed on each subinterface that is being used for AAL3/4 processing, and it must be an AAL3/4 virtual circuit.

Note ATM subinterfaces for SMDS networks are only supported on the AIP and NPM.

Support for AAL3/4 on an ATM interface requires static mapping of all protocols except IP. However, dynamic routing of IP can coexist with static mapping of other protocols on the same ATM interface.

After configuring the ATM interface for SMDS networks, configure the interface for standard protocol configurations, as needed. For more information about protocol configuration, refer to the relevant chapters of the Cisco IOS IP Configuration Guide , the Cisco IOS AppleTalk and Novell IPX Configuration Guide , and the Cisco IOS Apollo Domain , Banyan VINES , DECnet , ISO CLNS , and XNS Configuration Guide .

For examples of configuring an ATM interface for AAL3/4 support, see the section "Example ATM Interfaces for SMDS Encapsulation, on page 113" at the end of this chapter.

To configure an ATM interface for SMDS networks, use the following commands in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **atm aal aal3/4**
2. Router(config-if)# **atm smds-address** *address*
3. Router(config-if)# **atm multicast** *address*
4. Router(config-if)# **atm vp-filter** *hexvalue*
5. Router(config-if)# **pvc** [*name*] *vpi* / *vci* **smds**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **atm aal aal3/4**	Enables AAL3/4 support on the affected ATM subinterface.
Step 2	Router(config-if)# **atm smds-address** *address*	Provides an SMDS E.164 unicast address for the subinterface.
Step 3	Router(config-if)# **atm multicast** *address*	Provides an SMDS E.164 multicast address.
Step 4	Router(config-if)# **atm vp-filter** *hexvalue*	Configures a virtual path filter for the affected ATM subinterface. • The virtual path filter provides a mechanism for specifying which VPIs (or a range of VPIs) will be used for AAL3/4 processing during datagram reassembly. All other VPIs are mapped to AAL5 processing. For more information about the way the **atm vp-filter** command works and the effect of selecting specific values, refer to the *Cisco IOS Wide-Area Networking Command Reference*.
Step 5	Router(config-if)# **pvc** [*name*] *vpi* / *vci* **smds**	Creates an AAL3/4 PVC.

Limiting the Message Identifiers Allowed on Virtual Circuits

Message identifier (MID) numbers are used by receiving devices to reassemble cells from multiple sources into packets.

To ensure that the message identifiers are unique at the receiving end and, therefore, that messages can be reassembled correctly, you can limit the number of message identifiers allowed on a virtual circuit and assign different ranges of message identifiers to different PVCs.

To limit the number of message identifier numbers allowed on each virtual circuit and to assign different ranges of message identifiers to different PVCs, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **atm mid-per-vc** *maximum*
2. Router(config-if)# **pvc** [*name*] *vpi* / *vci* **smds**
3. Router(config-if-atm-vc)# **mid** *midlow midhigh*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **atm mid-per-vc** *maximum*	Limits the number of message identifiers allowed per virtual circuit. • The maximum number of message identifiers per virtual circuit is set at 16 by default; valid values are 16, 32, 64, 128, 256, 512, or 1024.
Step 2	Router(config-if)# **pvc** [*name*] *vpi* / *vci* **smds**	Creates an ATM PVC with SMDS encapsulation.
Step 3	Router(config-if-atm-vc)# **mid** *midlow midhigh*	Limits the range of message identifier values used on the PVC. • The default value for both the *midlow* and the *midhigh* arguments is zero.

Setting the Virtual Path Filter Register

The virtual path filter allows you to specify which VPI or range of VPIs will be used for AAL3/4 processing. The default value of the's virtual path filter register is 0x7B. To set the virtual path filter register, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **atm vp-filter** *hexvalue*	Sets the virtual path filter register.

Configuring Fast-Switched Transparent Bridging

The implementation of transparent bridging over ATM allows the spanning tree for an interface to support virtual circuit descriptors (VCDs) for AAL5-LLC Subnetwork Access Protocol (SNAP) encapsulations.

If the relevant interface or subinterface is explicitly put into a bridge group, as described in the task table below, AAL5-SNAP encapsulated bridge packets on a PVC are fast-switched.

The bridging implementation supports IEEE 802.3 frame formats, IEEE 802.10 frame formats, and Ethernet DIX frames. The router can accept IEEE 802.3 frames with or without frame check sequence (FCS). When the router receives frames with FCS (RFC 1483 bridge frame formats with 0x0001 in the PID field of the SNAP header), it strips off the FCS and forwards the frame as necessary. All IEEE 802.3 frames that originate at or are forwarded by the router are sent as 802.3 bridge frames without FCS (bridge frame formats with 0x0007 in the PID field of the SNAP header).

Note Transparent bridging for the ATM works only on AAL5-LLC/SNAP PVCs (fast-switched). AAL3/4-SMDS, AAL5-MUX, and AAL5-NLPID bridging are not yet supported. Transparent bridging for ATM also does not operate in a switched virtual circuit (SVC) environment.

No other configuration is required. Spanning tree updates are broadcast to all AAL5-SNAP virtual circuits that exist on the ATM interface. Only the AAL5-SNAP virtual circuits on the specific subinterface receive the updates. The router does not send spanning tree updates to AAL5-MUX and AAL5-NLPID virtual circuits.

For an example of transparent bridging for an AAL5-SNAP PVC, see the section "Example Transparent Bridging on an AAL5-SNAP PVC, on page 113" at the end of this chapter.

To configure transparent bridging for LLC/SNAP PVCs, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* **/0**[. *subinterface-number* {**multipoint** | **point-to-point**}]
2. Router(config-if)# **pvc**[*name*] *vpi* / *vci*
3. Router(config)# **exit**
4. Router(config-if)# **bridge-group** *group*
5. Router(config-if)# **exit**
6. Router(config)# **bridge** *group* **protocol dec**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**} • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0**[. *subinterface-number* {**multipoint** | **point-to-point**}]	Specifies the ATM interface using the appropriate format of the **interface atm** command.[14]

	Command or Action	Purpose
	Example: **Example:** **Example:** `Router(config)#` **interface atm** *number*`[`**.** *subinterface-number* `{`**multipoint** `|` **point-to-point**`}]`	
Step 2	Router(config-if)# **pvc**[*name*] *vpi* / *vci*	Creates one or more PVCs using AAL5-SNAP encapsulation. Repeat this command as needed.
Step 3	Router(config)# **exit**	Returns to interface configuration mode.
Step 4	Router(config-if)# **bridge-group** *group*	Assigns the interface to a bridge group.
Step 5	Router(config-if)# **exit**	Returns to global configuration mode.
Step 6	Router(config)# **bridge** *group* **protocol dec**	Defines the type of spanning tree protocol as DEC.

14 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring Inverse Multiplexing over ATM

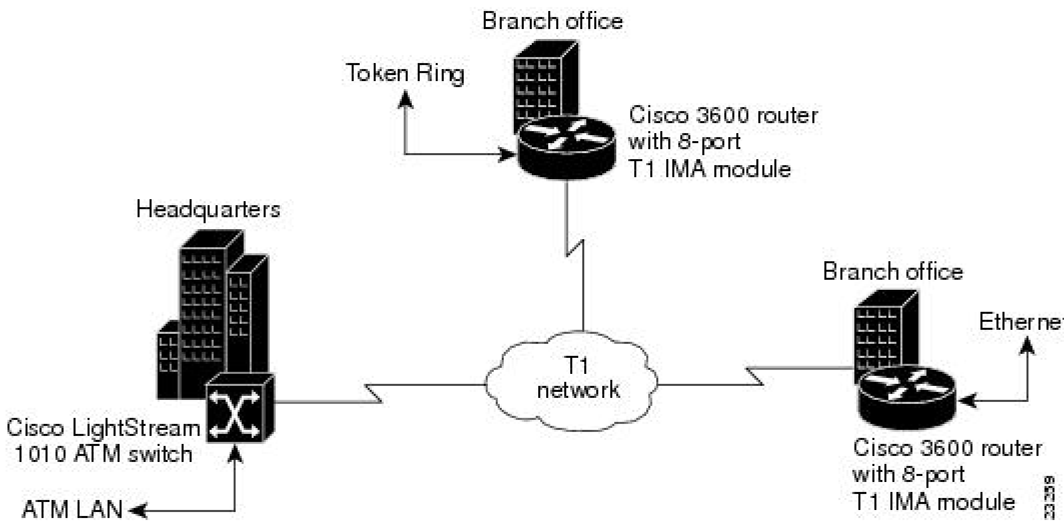
Inverse multiplexing provides the capability to transmit and receive a single high-speed data stream over multiple slower-speed physical links. In inverse multiplexing over ATM (IMA), the originating stream of ATM cells is divided so that complete ATM cells are transmitted in round-robin order across the set of ATM links.

IMA is supported on the Multiport T1/E1 ATM Network Module with Inverse Multiplexing over ATM on Cisco 2600 and Cisco 3600 series routers and the Multiport T1/E1 ATM Port Adapter with Inverse Multiplexing over ATM on Cisco 7100, Cisco 7200, and Cisco 7500 series routers. The Multiport T1/E1 ATM IMA network modules and port adapters provide four or eight T1 or E1 ports and allow wide-area networking (WAN) uplinks at speeds ranging from 1.536 Mbps to 12.288 Mbps for T1, and from 1.92 Mbps to 15.36 Mbps for E1. See the section Bandwidth Considerations, on page 75 later in this chapter for details.

Cisco's scalable ATM IMA solution means that you can deploy just the bandwidth you need by using multiple E1 or T1 connections instead of a more expensive E3, T3, or OC-3 to create links between LANs and ATM WAN applications. Enterprises and branch offices can aggregate traffic from multiple low-bandwidth digital physical transmission media, such as T1 pipes, to transmit voice and data at high-bandwidth connection speeds.

The figure below illustrates a scenario in which an organization must transport a mission-critical application among headquarters and branch offices at 6 Mbps.

Figure 3: LAN-to-WAN Application Connectivity with T1 and IMA



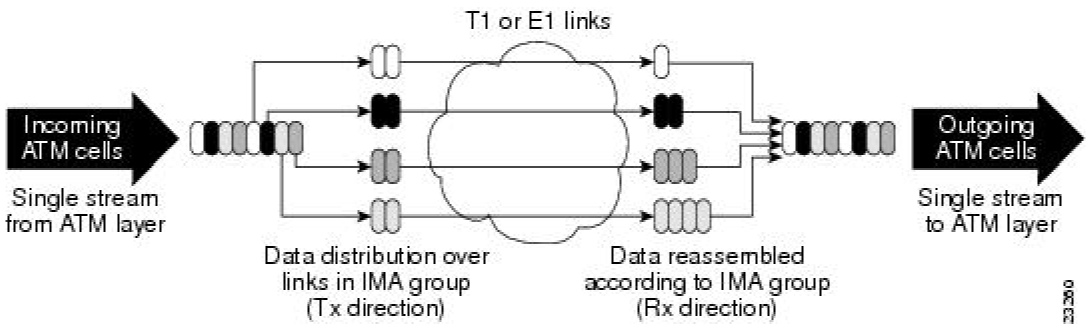
IMA Protocol Overview

In the transmit direction, IMA takes cells from the ATM layer and sends them in sequential distribution over the individual links that make up a logical link group called an IMA group (links can also be used individually instead of being a member of a group). The IMA group performance is approximately the sum of the links, although some overhead is required for ATM control cells. At the receiving end, the cells are recombined to form the original cell stream and are passed up to the ATM layer.

Filler cells are used to ensure a steady stream on the receiving side. IMA control protocol (ICP) cells control the operation of the inverse multiplexing function. With a frame length of 128, one of every 128 cells on each link is an ICP cell. The inverse multiplexing operation is transparent to the ATM layer protocols; therefore, the ATM layer can operate normally as if only a single physical interface were being used.

The figure below illustrates inverse multiplexing and demultiplexing with four bundled links, providing 6.144 Mbps of raw bandwidth for T1s and 7.68 Mbps of raw bandwidth for E1 for packet traffic. The transmit side, where cells are distributed across the links, is referred to as *Tx* , and the receive side, where cells are recombined, is called *Rx* .

Figure 4: Inverse Multiplexing and Demultiplexing



General Description of ATM T1 E1 IMA

ATM networks were designed to handle the demanding performance needs of voice, video, and data at broadband speeds of 34 Mbps and above. However, the high cost and spotty availability of long-distance broadband links limits broadband ATM WANs, preventing many organizations from taking advantage of the power of ATM. In response to these issues, the ATM Forum defined lower-speed ATM interface options for T1 and E1. However, this was not a complete solution because a single T1 or E1 link often does not provide enough bandwidth to support either traffic among different router and switch locations or heavy end-user demand.

For this reason, many organizations find themselves caught between the bandwidth limitations of a narrowband T1 or E1 line and the much higher costs of moving to broadband links. In response to this dilemma, the ATM Forum, with Cisco as an active member, defined Inverse Multiplexing for ATM (IMA). Using Cisco routers to provide ATM access gives branch offices and enterprises an affordable LAN-to-ATM interface.

For a list of ATM features that are supported on Cisco routers when you use the Multiport T1/E1 ATM Network Module with Inverse Multiplexing over ATM or the Multiport T1/E1 ATM Port Adapter with Inverse Multiplexing over ATM, see the "Cisco ATM Features" section of the "Wide-Area Networking Overview" chapter in this book.

Restrictions

IMA is supported on the following platforms:

- Cisco 2600 series and Cisco 3600 series routers using the Multiport T1/E1 Network Module with Inverse Multiplexing over ATM
- Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers using the Multiport T1/E1 ATM Port Adapter with Inverse Multiplexing over ATM

The following restrictions apply to the ATM IMA feature on Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers:

- If common transmit clock is configured on an IMA interface using the **ima clock-mode** command with the **common** keyword, then the port adapter internal clock is used as the transmit clock source for all the links of the IMA interface.

- The feature does not support the ATM real-time variable bit rate (rt-VBR) traffic category. The ATM constant bit rate (CBR) traffic category can be approximated by configuring a nonreal-time variable bit rate (nrt-VBR) VC with the same parameters for the sustainable cell rate (SCR) and peak cell rate (PCR).
- The following restrictions apply to SNMP:
  - IMA failure alarm trap is not supported.
  - Set operation for IMA MIB is not supported.
- The IP ATM_COS feature is not supported on Cisco 7500 series routers.

IMA Configuration Task List

The following sections describe the configuration and verification tasks required to set up ATM IMA groups. You can also configure ATM links individually, but these sections include only the steps for configuring IMA groups. To configure and verify IMA groups on an ATM interface, complete the tasks in the following sections. Each task is identified as optional or required.

For examples of IMA configuration, see the section "Examples Inverse Multiplexing over ATM, on page 113" at the end of this chapter.

Configuring an ATM Interface for IMA Operation

To configure the ATM interface for IMA operation, perform the tasks in one of the following two sections:

Configuring the Multiport T1 E1 ATM Network Module for IMA Operation

To configure an ATM interface on a Multiport T1/E1 ATM Network Module with Inverse Multiplexing over ATM for IMA operation, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot* / *port*
2. Router(config-if)# **clock source** {**line** | **internal** | {**loop-timed**}
3. Do one of the following:
   - Router(config-if)# **cablelength long** {**gain26** | **gain36**} {**-15db** | **-22.5db**| **-7.5db**| **0db**}
   -
   -
   - Router(config-if)# **cablelength short**{**133** | **266** | **399** | **533** | **655**}
4. Router(config-if)# **no ip address**
5. Router(config-if)# **no scrambling payload**
6. Router(config-if)# **impedance**{**75-ohm**|**120-ohm**}
7. Router(config-if)# **loopback** [**line** | **local** | **payload** | **remote**]
8. Router(config-if)# **fdl**{**att** | **ansi** | **all**| **none**}
9. Router(config-if)# **ima-group** *group-number*
10. Router(config-if)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot* / *port*	Enters interface configuration mode and specifies the location of the interface.
Step 2	Router(config-if)# **clock source** {**line** | **internal** | {**loop-timed**}	Sets the clock source for a link.
Step 3	Do one of the following: • Router(config-if)# **cablelength long** {**gain26** | **gain36**} {**-15db** | **-22.5db**| **-7.5db**| **0db**} • • • Router(config-if)# **cablelength short**{**133** | **266** | **399** | **533** | **655**}	(T1 interfaces only) Sets a cable length longer than 655 feet. (T1 interfaces only) Sets the cable length shorter than 655 feet.
Step 4	Router(config-if)# **no ip address**	Disables IP address configuration for the physical layer interface. This and other protocol parameters should be configured on the IMA interface instead of the T1/E1 interface.
Step 5	Router(config-if)# **no scrambling payload**	Randomizes the ATM cell payload frames to avoid continuous nonvariable bit patterns and improves the efficiency of ATM's cell delineation algorithms. By default, payload scrambling is on for E1 links and off for T1 links. Normally, the default setting for this command is sufficient.

	Command or Action	Purpose
Step 6	Router(config-if)# **impedance**{**75-ohm**|**120-ohm**}	(E1 interfaces only) Specifies the impedance (amount of wire resistance and reactivity to current) for the E1 link. The impedance is determined by the dongle-type cable that you plug in to the IMA module.
Step 7	Router(config-if)# **loopback** [**line** | **local** | **payload** | **remote**]	(For testing only) Loops all packets from the ATM interface back to the interface and directs the packets to the network.
Step 8	Router(config-if)# **fdl**{**att** | **ansi** | **all**| **none**}	(Optional, T1 only) Sets the Facility Data Link (FDL) exchange standard for the CSU controllers. The FDL is a 4-Kpbs channel used with the Extended SuperFrame (ESF) framing format to provide out-of-band messaging for error-checking on a T1 link. **Note** For T1, ESF framing and binary eight zero substitution (B8ZS) line encoding are set. For E1, CRC4 multiframe framing and HDB3 line encoding are set. These are the parameters specified by the ATM Forum, and they cannot be changed. You should generally leave this setting at the default, **ansi,**which follows the ANSI T1.403 standard for extended superframe facilities data link exchange support. Changing it allows improved management in some cases, but can cause problems if your setting is not compatible with that of your service provider.
Step 9	Router(config-if)# **ima-group** *group-number*	Specifies that the link is included in an IMA group. Enter an IMA group number from 0 to 3. You can specify up to four groups for each IMA network module. IMA groups usually span multiple ports on a module.
Step 10	Router(config-if)# **no shutdown**	Ensures that the link is active at the IMA level. If shut down, the link is added to the group, but put in an inhibited state.

Configuring the Multiport T1 E1 ATM Port Adapter for IMA Operation

To configure an ATM interface on a Multiport T1/E1 ATM Port Adapter with Inverse Multiplexing over ATM for IMA operation, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
    - Cisco 7100 series and 7200 series routers: Router(config)# **interface atm** *slot* / *port*
    - Cisco 7500 series: Router(config)# **interface atm** *slot* / *port-adapter* / *port*
2. Router(config-if)# **clock source**{**line**| **internal**}
3. Do one of the following:
    - Router(config-if)# **lbo long** {**gain26** | **gain36**} {**-15db** | **-22.5db**| **-7.5db**| **0db**}
    - **lbo short** {**133** | **266** | **399** | **533** | **655**}
4. Router(config-if)# **no ip address**
5. Router(config-if)# **no atm oversubscribe**
6. Router(config-if)# **no scrambling cell-payload**
7. Do one of the following:
    - For T1: Router(config-if)# **loopback** [**diagnostic**|**[payload**| **line**] | **remote**[**iboc**| **esf**[**payload**| **line**]]]
    - For E1: Router(config-if)# **loopback** [**diagnostic** | **local**[**payload**| **line**]]
8. Router(config-if)# **fdl**{**ansi**| **att**}
9. Router(config-if)# **ima-group** *group-number*
10. Router(config-if)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Cisco 7100 series and 7200 series routers: Router(config)# **interface atm** *slot* / *port* • Cisco 7500 series: Router(config)# **interface atm** *slot* / *port-adapter* / *port*	Enters interface configuration mode and specifies the location of the interface. • *slot* specifies the router slot position of the installed port adapter. Depending upon the router, enter a slot value from 1 to 5. • *port* specifies the T1 or E1 link that you are configuring. Enter a value from 0 to 7 for the eight ports. • *port-adapter* specifies on Cisco 7500 series routers the location of the port adapter on a VIP card. The Cisco IOS software creates the interfaces automatically when a port adapter is installed.
Step 2	Router(config-if)# **clock source**{**line**| **internal**}	Sets the clock source for a link. • **line** specifies that the link uses the recovered clock from the link and is the default setting. Generally, this setting is the most reliable. • **internal** specifies that the DS-1 link uses the internal clock.

	Command or Action	Purpose
		Note You should ensure that clock settings are properly configured for each link even when you intend to use a common link for clocking all the links in an IMA group.
Step 3	Do one of the following: • Router(config-if)# **lbo long** {**gain26** | **gain36**} {**-15db** | **-22.5db**| **-7.5db**| **0db**} • **lbo short** {**133** | **266** | **399** | **533** | **655**}	Sets a cable length of greater than 655 feet for a T1 link. • **gain26** specifies the decibel pulse gain at 26 decibels. This is the default pulse gain. • **gain36** specifies the decibel pulse gain at 36 decibels. • **-15db** specifies the decibel pulse rate at -15 decibels. • **-22.5db** specifies the decibel pulse rate at -22.5 decibels. • **-7.5db** specifies the decibel pulse rate at -7.5 decibels. • **0db** specifies the decibel pulse rate at 0 decibels. This is the default pulse rate. Sets a cable length of 655 feet or less for a T1 link. There is no default for **lbo short**. • **133** specifies a cable length from 0 to 133 feet. • **266** specifies a cable length from 134 to 266 feet. • **399** specifies a cable length from 267 to 399 feet. • **533** specifies a cable length from 400 to 533 feet. • **655** specifies a cable length from 534 to 655 feet. If you do not set the cable length, the system defaults to a setting of **lbo long gain26 0db**(space between **gain26** and **0db**).
Step 4	Router(config-if)# **no ip address**	Disables IP processing. • Instead of configuring protocol parameters on the physical interface, you can set these up on the IMA group virtual interface.
Step 5	Router(config-if)# **no atm oversubscribe**	Disables the ATM bandwidth manager, which keeps track of bandwidth used by virtual circuits on a per-interface basis. When you disable bandwidth manager, a check determines whether the ATM link is already oversubscribed. If it is, the command is rejected. Otherwise, the total bandwidth available on the link is recorded and all future connection setup requests are monitored to ensure that the link does not become oversubscribed.
Step 6	Router(config-if)# **no scrambling cell-payload**	Randomizes the ATM cell payload frames to avoid continuous nonvariable bit patterns and improve the efficiency of ATM cell delineation algorithms. Normally the default setting for this command is sufficient, with no specific command required. By default, scrambling is off for T1 or E1 links.
Step 7	Do one of the following: • For T1: Router(config-if)# **loopback** [**diagnostic**|[**payload**|	(For testing only) Loops all packets from the ATM interface back to the interface and directs the packets to the network. The default **line** setting places the interface into external loopback mode at the line.

	Command or Action	Purpose
	line] | **remote**[**iboc**| **esf**[**payload**| **line**]]] • For E1: Router(config-if)# **loopback** [**diagnostic** | **local**[**payload**| **line**]]	• **remote** sets the far end T1 interface into either payload or line loopback. • **local** loops the incoming receive signal back out of the transmitter. • **diagnostic** loops the outgoing transmit signal back to the receive signal.
Step 8	Router(config-if)# **fdl**{**ansi**| **att**}	(Optional) Sets the Facility Data Link (FDL) exchange standard for the Channel Service Unit (CSU) controllers. The FDL is a 4-Kbps channel used with the Extended Super Frame (ESF) framing format to provide out-of-band messaging for error-checking on a T1 link. Changing the default allows better management in some circumstances, but can cause problems if your setting is not compatible with that of your service provider.
Step 9	Router(config-if)# **ima-group** *group-number*	Specifies that the link is included in an IMA group. Enter an IMA group number from 0 to 3. You can specify up to four groups per IMA port adapter. IMA groups usually span multiple ports on a port adapter. • It is recommended that if the link is already a port of an IMA group then remove it from the IMA group both at the near end and far end and then move the link to a desired IMA group.
Step 10	Router(config-if)# **no shutdown**	Ensures that the link is active at the IMA level.

Verifying an ATM Interface Configured for IMA Operation

To verify that the ATM interface is configured correctly for IMA operation, perform the steps in one of the following sections:

Verifying the Multiport T1 E1 ATM Network Module for IMA Operation

Follow the steps below to verify the configuration of an ATM interface on a Multiport T1/E1 ATM Network Module.

SUMMARY STEPS

1. To verify the configuration of an ATM interface, enter the **show interface atm** command. Notice that the total count of configured virtual circuits (VCs) is shown.
2. To get information about the physical link, enter the **show controller atm** command.

DETAILED STEPS

Step 1 To verify the configuration of an ATM interface, enter the **show interface atm** command. Notice that the total count of configured virtual circuits (VCs) is shown.

Example:

```
Router# show interface atm 0/1
ATM0/1 is up, line protocol is up
  Hardware is ATM T1
  Internet address is 10.1.1.2/8
  MTU 4470 bytes, sub MTU 4470, BW 1500 Kbit, DLY 20000 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s): AAL5
  256 maximum active VCs, 3 current VCCs
  VC idle disconnect time: 300 seconds
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Step 2 To get information about the physical link, enter the **show controller atm** command.

Example:

```
Router# show controller atm0/2
Interface ATM0/2 is administratively down
  Hardware is ATM T1
LANE client MAC address is 0050.0f0c.1482
  hwidb=0x617BEE9C, ds=0x617D498C
  slot 0, unit 2, subunit 2
  rs8234 base 0x3C000000, slave base 0x3C000000
  rs8234 ds 0x617D498C
  SBDs - avail 2048, guaranteed 2, unguaranteed 2046, starved 0
 Seg VCC table 3C00B800, Shadow Seg VCC Table 617EF76C, VCD Table 61805798
 Schedule table 3C016800, Shadow Schedule table 618087C4, Size 63D
 RSM VCC Table 3C02ED80, Shadow RSM VCC Table 6180C994
 VPI Index Table 3C02C300, VCI Index Table 3C02E980
 Bucket2 Table 3C01E500, Shadow Bucket2 Table 6180A0E4
 MCR Limit Table 3C01E900, Shadow MCR Table 617D2160
 ABR template 3C01EB00, Shadow template 614DEEAC
 RM Cell RS Queue 3C02C980
 Queue           TXQ Addr  Pos  StQ Addr  Pos
 0  UBR CHN0     3C028B00  0    03118540  0
 1  UBR CHN1     3C028F00  0    03118D40  0
 2  UBR CHN2     3C029300  0    03119540  0
 3  UBR CHN3     3C029700  0    03119D40  0
 4  VBR/ABR CHN0 3C029B00  0    0311A540  0
 5  VBR/ABR CHN1 3C029F00  0    0311AD40  0
 6  VBR/ABR CHN2 3C02A300  0    0311B540  0
 7  VBR/ABR CHN3 3C02A700  0    0311BD40  0
 8  VBR-RT CHN0  3C02AB00  0    0311C540  0
 9  VBR-RT CHN1  3C02AF00  0    0311CD40  0
 10 VBR-RT CHN2  3C02B300  0    0311D540  0
 11 VBR-RT CHN3  3C02B700  0    0311DD40  0
 12 SIG          3C02BB00  0    0311E540  0
```

```
 13 VPD          3C02BF00  0    0311ED40  0

 Queue           FBQ Addr  Pos  RSQ Addr  Pos
 0  OAM          3C0EED80  255  0311F600  0
 1  UBR CHN0     3C0EFD80  0    03120600  0
 2  UBR CHN1     3C0F0D80  0    03121600  0
 3  UBR CHN2     3C0F1D80  0    03122600  0
 4  UBR CHN3     3C0F2D80  0    03123600  0
 5  VBR/ABR CHN0 3C0F3D80  0    03124600  0
 6  VBR/ABR CHN1 3C0F4D80  0    03125600  0
 7  VBR/ABR CHN2 3C0F5D80  0    03126600  0
 8  VBR/ABR CHN3 3C0F6D80  0    03127600  0
 9  VBR-RT CHN0  3C0F7D80  0    03128600  0
 10 VBR-RT CHN1  3C0F8D80  0    03129600  0
 11 VBR-RT CHN2  3C0F9D80  0    0312A600  0
 12 VBR-RT CHN3  3C0FAD80  0    0312B600  0
 13 SIG          3C0FBD80  255  0312C600  0
SAR Scheduling channels:  -1 -1 -1 -1 -1 -1 -1 -1
Part of IMA group 3
Link 2 IMA Info:
   group index is 1
   Tx link id is 2, Tx link state is unusableNoGivenReason
   Rx link id is 99, Rx link state is unusableFault
    Rx link failure status is fault,
    0 tx failures, 3 rx failures
Link 2 Framer Info:
    framing is ESF, line code is B8ZS, fdl is ANSI
    cable-length is long, Rcv gain is 26db and Tx gain is 0db,
    clock src is line, payload-scrambling is disabled, no loopback
    line status is 0x1064; or Tx RAI, Rx LOF, Rx LOS, Rx LCD.
    port is active, link is unavailable
    0 idle rx, 0 correctable hec rx, 0 uncorrectable hec rx
    0 cells rx, 599708004 cells tx, 0 rx fifo overrun.
Link (2):DS1 MIB DATA:
  Data in current interval (518 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 518 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 519 Unavail Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 86400 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 86400 Unavail Secs
SAR counter totals across all links and groups:
   0 cells output, 0 cells stripped
   0 cells input, 0 cells discarded, 0 AAL5 frames discarded
   0 pci bus err, 0 dma fifo full err, 0 rsm parity err
   0 rsm syn err, 0 rsm/seg q full err, 0 rsm overflow err
   0 hs q full err, 0 no free buff q err, 0 seg underflow err
   0 host seg stat q full err
```

Verifying the Multiport T1 E1 ATM Port Adapter for IMA Operation

Follow the steps below to verify configuration of an ATM interface on a Multiport T1/E1 ATM Port Adapter.

SUMMARY STEPS

1. Use the privileged EXEC **show interface atm** *slot*/*port*command to verify configuration of the ATM interface. Note that the total count of configured VCs is shown.
2. To get information about the physical link, use the privileged EXEC **show controller**[**atm**[*slot*/*port*]] command.

DETAILED STEPS

Step 1 Use the privileged EXEC **show interface atm** *slot*/*port*command to verify configuration of the ATM interface. Note that the total count of configured VCs is shown.

Example:

```
Router# show interface atm 5/0
ATM5/0 is up, line protocol is up
  Hardware is IMA PA
  Internet address is 10.0.2.0/16
  MTU 4470 bytes, sub MTU 4470, BW 1536 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5
  512 maximum active VCs, 3 current VCCs
  VC idle disconnect time:300 seconds
  1 carrier transitions
  Last input 00:43:16, output 00:43:16, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4803 packets input, 5928671 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4823 packets output, 5911619 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Step 2 To get information about the physical link, use the privileged EXEC **show controller**[**atm**[*slot*/*port*]] command.

Example:

```
Router# show controller atm 1/ima0
Interface ATM1/ima0 is up
Hardware is IMA PA - DS1 (1Mbps)
Framer is PMC PM7344, SAR is LSI ATMIZER II
Firmware rev:G102, ATMIZER II rev:3
  idb=0x61DE9F10, ds=0x6185C0A0, vc=0x6187D3C0, pa=0x6184AF40
  slot 1, unit 9, subunit 0, fci_type 0x00BA, ticks 701720
  400 rx buffers:size=512, encap=64, trailer=28, magic=4
Curr Stats:
  rx_cell_lost=0, rx_no_buffer=0, rx_crc_10=0
  rx_cell_len=0, rx_no_vcd=0, rx_cell_throttle=0, tx_aci_err=0
Rx Free Ring status:
  base=0x3CFF0040, size=1024, write=320
Rx Compl Ring status:
  base=0x338DCE40, size=2048, read=1275
Tx Ring status:
  base=0x3CFE8040, size=8192, write=700
Tx Compl Ring status:
  base=0x338E0E80, size=2048, read=344
BFD Cache status:
  base=0x61878340, size=5120, read=5107
Rx Cache status:
  base=0x61863D80, size=16, write=11
Tx Shadow status:
  base=0x618641C0, size=8192, read=687, write=700
Control data:
  rx_max_spins=12, max_tx_count=25, tx_count=13
```

```
  rx_threshold=267, rx_count=11, tx_threshold=3840
  tx bfd write indx=0x27, rx_pool_info=0x61863E20
Control data base address:
       rx_buf_base = 0x038A15A0        rx_p_base = 0x6185CB40
            rx_pak = 0x61863AF0              cmd = 0x6185C320
       device_base = 0x3C800000     ima_pa_stats = 0x038E2FA0
        sdram_base = 0x3CE00000       pa_cmd_buf = 0x3CFFFC00
       vcd_base[0] = 0x3CE3C100      vcd_base[1] = 0x3CE1C000
         chip_dump = 0x038E3D7C       dpram_base = 0x3CD80000
   sar_buf_base[0] = 0x3CE4C000  sar_buf_base[1] = 0x3CF22000
       bfd_base[0] = 0x3CFD4000      bfd_base[1] = 0x3CFC0000
       acd_base[0] = 0x3CE88360      acd_base[1] = 0x3CE5C200
     pci_atm_stats = 0x038E2EC0
ATM1/ima0 is up
        hwgrp number = 1
grp tx up reg= 0x5, grp rx up reg= 0x3, rx dcb reg= 0xD4 0x4, tx links grp reg=
0x3, scci reg= 0x3C, ima id reg= 0x0, group status  reg= 0xA2, tx timing reg= 0x
20, tx test reg= 0x21, tx test pattern reg= 0x41, rx test pattern reg= 0x42, icp
 cell link info  reg= 0xFC, icp cell link info  reg= 0xFC, icp cell link info  r
eg= 0x0, icp cell link info  reg= 0x0, icp cell link info  reg= 0x0, icp cell li
nk info  reg= 0x0, icp cell link info  reg= 0x0, icp cell link info  reg= 0x0
```

Configuring IMA Groups

As shown in the previous section, the **ima-group** command configures links on an ATM interface as IMA group members. When IMA groups have been set up in this way, you can configure settings for each group. To configure IMA groups and settings for each group, perform the tasks in one of the following two sections:

Configuring IMA Groups on the Multiport T1 E1 ATM Network Module

To configure IMA groups and settings for each group on the Multiport T1/E1 ATM Network Module with Inverse Multiplexing over ATM, use following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot*/**ima** *group-number*
2. Router(config-if)# **ip address** *ip-address*
3. Router(config-if)# **no atm oversubscribe**
4. Router(config-if)# **pvc** [*name*] *vpi* / *vci* **ilmi**
5. Router(config-if-atm-vc)# **exit**
6. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
7. Router (config-if-atm-vc)# **protocol ip** *address* **broadcast**
8. Router (config-if-atm-vc)# **vbr-rt** *peak-rate average-rate burst*
9. Router (config-if-atm-vc)# **exit**
10. Router(config-if)# **ima clock-mode** {**common**[*port*] | {**independent**}
11. Router(config-if)# **ima active-links-minimum** *number*
12. Router(config-if)# **ima differential-delay-maximum** *msec*
13. Router(config-if)# **ima test** [**link** *port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot*/**ima** *group-number*	Enters interface configuration mode and specifies the slot location of the interface and IMA group number. • *slot* indicates the router slot where the port adapter is located. • *group-number* is the IMA group label. There should be no space between "**ima**" and the group number.
Step 2	Router(config-if)# **ip address** *ip-address*	Sets protocol parameters for the whole group.
Step 3	Router(config-if)# **no atm oversubscribe**	Disables the ATM bandwidth manager, which keeps track of bandwidth used by virtual circuits on a per-interface basis. When you disable bandwidth manager, a check determines whether the ATM link is already oversubscribed. If it is, the command is rejected. Otherwise, the total bandwidth available on the link is recorded and all future connection setup requests are monitored to ensure that the link does not become oversubscribed.
Step 4	Router(config-if)# **pvc** [*name*] *vpi* / *vci* **ilmi**	Creates an ATM PVC for ILMI management purposes and enters Interface-ATM-VC configuration mode.
Step 5	Router(config-if-atm-vc)# **exit**	Exits Interface-ATM-VC configuration mode.
Step 6	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Enables a PVC.
Step 7	Router (config-if-atm-vc)# **protocol ip** *address* **broadcast**	Specifies a protocol address for the PVC. **Note** The default AAL5 layer and SNAP encapsulation is used in this example, so the **encapsulation aal5** *encap* command is unnecessary.
Step 8	Router (config-if-atm-vc)# **vbr-rt** *peak-rate average-rate burst*	Configures a type of ATM service on the PVC. This example uses Variable Bit Rate, real-time, for AAL5 communications, allowing you to set different cell rate parameters for connections where there is a fixed timing relationship among samples. (VBR is generally used with AAL5 and IP over ATM.) The command configures traffic shaping so that the carrier does not discard calls. Configures the burst value if the PVC will carry bursty traffic.
Step 9	Router (config-if-atm-vc)# **exit**	Exits Interface-ATM-VC configuration mode and returns to interface configuration mode.
Step 10	Router(config-if)# **ima clock-mode** {**common**[*port*] | {**independent**}	Sets the transmit clock mode for the group.
Step 11	Router(config-if)# **ima active-links-minimum** *number*	Specifies how many transmit links must be active in order for the IMA group to be operational.
Step 12	Router(config-if)# **ima differential-delay-maximum** *msec*	Specifies the maximum allowed differential timing delay that can exist among the active links in an IMA group.

	Command or Action	Purpose
Step 13	Router(config-if)# **ima test** [**link** *port*] **Example:** [**pattern** *pattern-id*]	Starts the IMA link test procedure with the specified link and pattern.

Configuring IMA Groups on the Multiport T1 E1 ATM Port Adapter

To configure IMA groups and settings for each group on the Multiport T1/E1 ATM Port Adapter with Inverse Multiplexing over ATM, use following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
    - Router(config)# **interface atm** *slot*/**ima** *group number*
    -
    - (Cisco 7100 series and 7200 series routers)
    -
    - Router(config)# **interface atm** *slot* / *port-adapter* / **ima** *group number*
2. Router(config-if)# **ip address** *ip-address*
3. Router(config-if)# **pvc** *vpi*/*vci* **ilmi**
4. Router (config-if-atm-vc)# **pvc** *vpi*/*vci* **qsaal**
5. Router (config-if-atm-vc)# **exit**
6. Router (config-if)# **svc** *name* **nsap** *nsap-address*
7. Router (config-if-atm-vc)# **protocol ip** *address* **broadcast**
8. Router (config-if-atm-vc)# **exit**
9. Router(config-if)# **ima clock-mode**{**common**[*port*] | **independent**}[17]
10. Router(config-if)# **ima active-links-minimum** *number*
11. Router(config-if)# **ima differential-delay-maximum** *msec*
12. Router(config-if)# **ima test**[**link** *port*] [**pattern** *pattern-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot*/**ima** *group number*	Enters interface configuration mode and specifies the slot location of the interface and IMA group number.

	Command or Action	Purpose
	• • (Cisco 7100 series and 7200 series routers) • • Router(config)# **interface atm** *slot* / *port-adapter* / **ima** *group number* **Example:** **Example:** `(Cisco 7500 series routers)` **Example:**	• *slot* indicates the router slot where the port adapter is located. Depending upon the router, enter a slot value from 1 to 5. • *group-number* is the IMA group label. Enter a value from 0 to 3. There should be no space between "**ima**" and the group number. • *port-adapter* indicatesthe physical port adapter slot on the VIP2. • *port* identifies the interface port on the IMA port adapter.
Step 2	Router(config-if)# **ip address** *ip-address*	Sets protocol parameters for the whole group.
Step 3	Router(config-if)# **pvc** *vpi*/*vci* **ilmi**	Creates an ATM PVC for ILMI management purposes and enters VC configuration mode. To set up communication with the ILMI, use a value of **ilmi** for ATM adaptation layer encapsulation; the associated *vpi* and *vci* values are ordinarily 0 and 16, respectively.
Step 4	Router (config-if-atm-vc)# **pvc** *vpi*/*vci* **qsaal**	Enables the signaling for setup and teardown of SVCs by specifying the Q.SAAL[15] encapsulations; the associated *vpi* and *vci* values are ordinarily 0 and 5, respectively. **Note** You can also set up PVCs for sending information.
Step 5	Router (config-if-atm-vc)# **exit**	To complete configuration of a PVC, exit VC configuration mode.
Step 6	Router (config-if)# **svc** *name* **nsap** *nsap-address*	Sets up SVCs for sending ATM information. Once you specify a name for an SVC, you can reenter the interface-ATM-VC configuration mode by simply entering **svc** *name.* *nsap-address* is a 40-digit hexadecimal number.
Step 7	Router (config-if-atm-vc)# **protocol ip** *address* **broadcast**	Specifies a protocol address for the SVC. **Note** The default AAL5 layer and SNAP[16] encapsulation are used in this example, so the **encapsulation** *aalencap* command is unnecessary.
Step 8	Router (config-if-atm-vc)# **exit**	Exits VC configuration mode and returns to interface configuration mode.

	Command or Action	Purpose
Step 9	Router(config-if)# **ima clock-mode**{**common**[*port*] | **independent**}[17]	Sets the transmit clock mode for the group. If all the links in the group should share a clock source, use the **common** keyword. If each link uses a different clock source, use the **independent** clock source keyword. Using the *port* keyword, you can specify a link for common clocking. The default uses the common clock as the transmit clock source.
Step 10	Router(config-if)# **ima active-links-minimum** *number*	When used with a number value from 1 to 8, specifies how many transmit links must be active in order for the IMA group to be operational. The setting you choose depends on your performance requirements as well as on the total number of links in the group. If fewer than the preset minimum are active, the group is automatically rendered inactive until the minimum number of links is up again. The default value is 1.
Step 11	Router(config-if)# **ima differential-delay-maximum** *msec*	Specifies the differential timing delay among the links in an IMA group by entering a milliseconds value from 25 to 250 for T1 and 25 to 190 for E1. If a link delay exceeds the specified maximum, the link is dropped; otherwise, the IMA feature adjusts for differences in delays so that all links in a group are aligned. A shorter value provides less resiliency in adjusting for variations than a higher value. However, a higher value might affect overall group performance because increased differential delay adds more latency to the traffic that is transmitted across the group.
Step 12	Router(config-if)# **ima test**[**link** *port*] [**pattern** *pattern-id*] **Example:**	(For testing only) Troubleshoots or diagnoses physical link connectivity. The IMA feature performs ongoing tests on all links in a group, to verify link connectivity. Use this command to specify both a link to use for testing and as a test pattern. The pattern is sent from the specified link and looped back from the receiving end in the multiplexing-demultiplexing process. A byte in the ICP cell identifies the pattern.

15 Q Signaling ATM adaptation Layer.

16 Subnetwork Access Protocol.

17 To form an IMA group with independent clock mode, use the no shut command in the IMA interface only. To change the mode to independent from an already existing IMA group, use the no ima command on the IMA group links. Next, change the mode, add all the links, and then issue the no shut command in the IMA interface.

Verifying IMA Group Configuration

To verify IMA group configuration, perform the steps in one of the following two sections:

Verifying IMA Group Configuration on the Multiport T1 E1 ATM Network Module

Perform the following steps to verify IMA group configuration on the Multiport T1/E1 ATM Network Module.

SUMMARY STEPS

1. To display information about IMA group interfaces, enter the **show ima interface atm** command. The first example shows the command output without the **detail** keyword; the second example shows the detailed information.
2. To review physical level information about the IMA group, enter the **show controllers atm**command in privileged EXEC mode, as shown in the following example:
3. To see how SVCs and PVCs are set up, enter the privileged EXEC **show atm vc** command.

DETAILED STEPS

Step 1 To display information about IMA group interfaces, enter the **show ima interface atm** command. The first example shows the command output without the **detail** keyword; the second example shows the detailed information.

Example:

```
Router# show ima interface atm2/ima2
Interface ATM2/IMA2 is up
        Group index is 2
        Ne state is operational, failure status is noFailure
        active links bitmap 0x30
    IMA Group Current Configuration:
        Tx/Rx configured links bitmap 0x30/0x30
        Tx/Rx minimum required links 1/1
        Maximum allowed diff delay is 25ms, Tx frame length 128
        Ne Tx clock mode CTC, configured timing reference link ATM2/4
        Test pattern procedure is disabled
    IMA Group Current Counters (time elapsed 12 seconds):
        3 Ne Failures, 3 Fe Failures, 4 Unavail Secs
    IMA Group Total Counters (last 0 15 minute intervals):
        0 Ne Failures, 0 Fe Failures, 0 Unavail Secs
    IMA link Information:
        Link     Physical Status        NearEnd Rx Status      Test Status
        ----     ---------------        -----------------      -----------
        ATM2/4   up                     active                 disabled
        ATM2/5   up                     active                 disabled
router# show ima interface atm2/ima2 detail
Interface ATM2/IMA2 is up
        Group index is 2
        Ne state is operational, failure status is noFailure
        active links bitmap 0x30
    IMA Group Current Configuration:
        Tx/Rx configured links bitmap 0x30/0x30
        Tx/Rx minimum required links 1/1
        Maximum allowed diff delay is 25ms, Tx frame length 128
        Ne Tx clock mode CTC, configured timing reference link ATM2/4
        Test pattern procedure is disabled
    Detailed group Information:
        Tx/Rx Ima_id 0x22/0x40, symmetry symmetricOperation
        Number of Tx/Rx configured links 2/2
        Number of Tx/Rx active links 2/2
        Fe Tx clock mode ctc, Rx frame length 128
        Tx/Rx timing reference link 4/4
        Maximum observed diff delay 0ms, least delayed link 5
        Running seconds 32
        GTSM last changed 10:14:41 UTC Wed Jun 16 1999
    IMA Group Current Counters (time elapsed 33 seconds):
        3 Ne Failures, 3 Fe Failures, 4 Unavail Secs
    IMA Group Total Counters (last 0 15 minute intervals):
        0 Ne Failures, 0 Fe Failures, 0 Unavail Secs
    Detailed IMA link Information:

Interface ATM2/4 is up
```

```
        ifIndex 13, Group Index 2, Row Status is active
        Tx/Rx Lid 4/4, relative delay 0ms
        Ne Tx/Rx state active/active
        Fe Tx/Rx state active/active
        Ne Rx failure status is noFailure
        Fe Rx failure status is noFailure
        Rx test pattern 0x41, test procedure disabled
    IMA Link Current Counters (time elapsed 35 seconds):
        1 Ima Violations, 0 Oif Anomalies
        1 Ne Severely Err Secs, 2 Fe Severely Err Secs
        0 Ne Unavail Secs, 0 Fe Unavail Secs
        2 Ne Tx Unusable Secs, 2 Ne Rx Unusable Secs
        0 Fe Tx Unusable Secs, 2 Fe Rx Unusable Secs
        0 Ne Tx Failures, 0 Ne Rx Failures
        0 Fe Tx Failures, 0 Fe Rx Failures
    IMA Link Total Counters (last 0 15 minute intervals):
        0 Ima Violations, 0 Oif Anomalies
        0 Ne Severely Err Secs, 0 Fe Severely Err Secs
        0 Ne Unavail Secs, 0 Fe Unavail Secs
        0 Ne Tx Unusable Secs, 0 Ne Rx Unusable Secs
        0 Fe Tx Unusable Secs, 0 Fe Rx Unusable Secs
        0 Ne Tx Failures, 0 Ne Rx Failures
        0 Fe Tx Failures, 0 Fe Rx Failures

Interface ATM2/5 is up
        ifIndex 14, Group Index 2, Row Status is active
        Tx/Rx Lid 5/5, relative delay 0ms
        Ne Tx/Rx state active/active
        Fe Tx/Rx state active/active
        Ne Rx failure status is noFailure
        Fe Rx failure status is noFailure
        Rx test pattern 0x41, test procedure disabled
    IMA Link Current Counters (time elapsed 46 seconds):
        1 Ima Violations, 0 Oif Anomalies
        1 Ne Severely Err Secs, 2 Fe Severely Err Secs
        0 Ne Unavail Secs, 0 Fe Unavail Secs
        2 Ne Tx Unusable Secs, 2 Ne Rx Unusable Secs
        0 Fe Tx Unusable Secs, 2 Fe Rx Unusable Secs
        0 Ne Tx Failures, 0 Ne Rx Failures
        0 Fe Tx Failures, 0 Fe Rx Failures
    IMA Link Total Counters (last 0 15 minute intervals):
        0 Ima Violations, 0 Oif Anomalies
        0 Ne Severely Err Secs, 0 Fe Severely Err Secs
        0 Ne Unavail Secs, 0 Fe Unavail Secs
        0 Ne Tx Unusable Secs, 0 Ne Rx Unusable Secs
        0 Fe Tx Unusable Secs, 0 Fe Rx Unusable Secs
        0 Ne Tx Failures, 0 Ne Rx Failures
        0 Fe Tx Failures, 0 Fe Rx Failures
```

Step 2 To review physical level information about the IMA group, enter the **show controllers atm**command in privileged EXEC mode, as shown in the following example:

Example:

```
router# show controllers atm0/ima3
Interface ATM0/IMA3 is up
  Hardware is ATM IMA
  LANE client MAC address is 0050.0f0c.148b
  hwidb=0x61C2E990, ds=0x617D498C
  slot 0, unit 3, subunit 3
  rs8234 base 0x3C000000, slave base 0x3C000000
  rs8234 ds 0x617D498C
  SBDs - avail 2048, guaranteed 3, unguaranteed 2045, starved 0
 Seg VCC table 3C00B800, Shadow Seg VCC Table 617EF76C, VCD Table 61805798
 Schedule table 3C016800, Shadow Schedule table 618087C4, Size 63D
 RSM VCC Table 3C02ED80, Shadow RSM VCC Table 6180C994
 VPI Index Table 3C02C300, VCI Index Table 3C02E980
 Bucket2 Table 3C01E500, Shadow Bucket2 Table 6180A0E4
 MCR Limit Table 3C01E900, Shadow MCR Table 617D2160
```

```
 ABR template 3C01EB00, Shadow template 614DEEAC
 RM Cell RS Queue 3C02C980
 Queue           TXQ Addr  Pos  StQ Addr  Pos
 0  UBR CHN0     3C028B00  0    03118540  0
 1  UBR CHN1     3C028F00  0    03118D40  0
 2  UBR CHN2     3C029300  0    03119540  0
 3  UBR CHN3     3C029700  0    03119D40  0
 4  VBR/ABR CHN0 3C029B00  0    0311A540  0
 5  VBR/ABR CHN1 3C029F00  0    0311AD40  0
 6  VBR/ABR CHN2 3C02A300  0    0311B540  0
 7  VBR/ABR CHN3 3C02A700  0    0311BD40  0
 8  VBR-RT CHN0  3C02AB00  0    0311C540  0
 9  VBR-RT CHN1  3C02AF00  0    0311CD40  0
 10 VBR-RT CHN2  3C02B300  0    0311D540  0
 11 VBR-RT CHN3  3C02B700  0    0311DD40  0
 12 SIG          3C02BB00  0    0311E540  0
 13 VPD          3C02BF00  0    0311ED40  0

 Queue           FBQ Addr  Pos  RSQ Addr  Pos
 0  OAM          3C0EED80  255  0311F600  0
 1  UBR CHN0     3C0EFD80  0    03120600  0
 2  UBR CHN1     3C0F0D80  0    03121600  0
 3  UBR CHN2     3C0F1D80  0    03122600  0
 4  UBR CHN3     3C0F2D80  0    03123600  0
 5  VBR/ABR CHN0 3C0F3D80  0    03124600  0
 6  VBR/ABR CHN1 3C0F4D80  0    03125600  0
 7  VBR/ABR CHN2 3C0F5D80  0    03126600  0
 8  VBR/ABR CHN3 3C0F6D80  0    03127600  0
 9  VBR-RT CHN0  3C0F7D80  0    03128600  0
 10 VBR-RT CHN1  3C0F8D80  255  03129600  0
 11 VBR-RT CHN2  3C0F9D80  0    0312A600  0
 12 VBR-RT CHN3  3C0FAD80  0    0312B600  0
 13 SIG          3C0FBD80  255  0312C600  0
SAR Scheduling channels:  -1 -1 -1 -1 -1 -1 -1 -1
ATM channel number is 1
link members are 0x7, active links are 0x0
Group status is blockedNe, 3 links configured,
Group Info: Configured links bitmap 0x7, Active links bitmap 0x0,
    Tx/Rx IMA_id 0x3/0x63,
    NE Group status is startUp,
    frame length 0x80, Max Diff Delay 0,
    1 min links, clock mode ctc, symmetry symmetricOperation, trl 0,
    Group Failure status is startUpNe.
    Test pattern procedure is disabled
SAR counter totals across all links and groups:
   0 cells output, 0 cells stripped
   0 cells input, 0 cells discarded, 0 AAL5 frames discarded
   0 pci bus err, 0 dma fifo full err, 0 rsm parity err
   0 rsm syn err, 0 rsm/seg q full err, 0 rsm overflow err
   0 hs q full err, 0 no free buff q err, 0 seg underflow err
   0 host seg stat q full err
```

Step 3 To see how SVCs and PVCs are set up, enter the privileged EXEC **show atm vc** command.

Example:

```
 VCD /                                       Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells  Sts
0/1        1            0    50   PVC    SNAP     UBR    1000                INAC
0/IMA3     2            0     5   PVC    SAAL     UBR    4000                  UP
0/IMA3     3            0    16   PVC    ILMI     UBR    4000                  UP
0/IMA3     first        1    13   PVC    MUX      VBR     640    320   80      UP
0/IMA3     4            0    34   SVC    SNAP     VBR-RT  768    768           UP
```

Verifying IMA Group Configuration on the Multiport T1 E1 ATM Port Adapter

Perform the following steps to verify IMA group configuration on the Multiport T1/E1 ATM Port Adapter.

SUMMARY STEPS

1. To display information about IMA group interfaces, use the **show ima interface atm** command in privileged EXEC mode. First, the group information appears. Then, information about each link in the group (there are two in this example) is displayed under "IMA Detailed Link Information."
2. To see how SVCs and PVCs are set up, use the **show atm vc** command in privileged EXEC mode.

DETAILED STEPS

Step 1 To display information about IMA group interfaces, use the **show ima interface atm** command in privileged EXEC mode. First, the group information appears. Then, information about each link in the group (there are two in this example) is displayed under "IMA Detailed Link Information."

Note If you do not enter the **detail**keyword, you do not see the IMA MIB information or the "Detailed Link Information" output displayed in the example below.

Example:

```
Router# show ima interface atm 1/ima0 detail
ATM1/ima0 is up
        ImaGroupState:NearEnd = operational, FarEnd = operational
        ImaGroupFailureStatus  = noFailure
IMA Group Current Configuration:
        ImaGroupMinNumTxLinks = 2    ImaGroupMinNumRxLinks = 2
        ImaGroupDiffDelayMax  = 25   ImaGroupNeTxClkMode   = common(ctc)
        ImaGroupFrameLength   = 128  ImaTestProcStatus     = disabled
        ImaGroupTestLink      = 0    ImaGroupTestPattern   = 0xFF
IMA MIB Information:
        ImaGroupSymmetry        = symmetricOperation
        ImaGroupFeTxClkMode     = common(ctc)
        ImaGroupRxFrameLength   = 128
        ImaGroupTxTimingRefLink = 0     ImaGroupRxTimingRefLink = 0
        ImaGroupTxImaId         = 0     ImaGroupRxImaId         = 0
        ImaGroupNumTxCfgLinks   = 2     ImaGroupNumRxCfgLinks   = 2
        ImaGroupNumTxActLinks   = 2     ImaGroupNumRxActLinks   = 2
        ImaGroupLeastDelayLink  = 1     ImaGroupDiffDelayMaxObs = 0
IMA group counters:
        ImaGroupNeNumFailures   = 78    ImaGroupFeNumFailures   = 68
        ImaGroupUnAvailSecs     = 441453        ImaGroupRunningSecs     =
445036
IMA Detailed Link Information:
ATM1/0 is up
        ImaLinkRowStatus = LinkRowStatusUnknown
        ImaLinkIfIndex   = 0            ImaLinkGroupIndex = 0
        ImaLinkState:
                NeTx = active
                NeRx = active
                FeTx = active
                FeRx = active
        ImaLinkFailureStatus:
                NeRx = noFailure
                FeRx = noFailure
        ImaLinkTxLid           = 0      ImaLinkRxLid           = 0
        ImaLinkRxTestPattern   = 65     ImaLinkTestProcStatus  = disabled
        ImaLinkRelDelay        = 0
IMA Link counters :
        ImaLinkImaViolations   = 1
        ImaLinkNeSevErroredSec = 41     ImaLinkFeSevErroredSec = 34
```

```
        ImaLinkNeUnavailSec    = 441505 ImaLinkFeUnAvailSec    = 28
        ImaLinkNeTxUnusableSec = 2      ImaLinkNeRxUnUsableSec = 441542
        ImaLinkFeTxUnusableSec = 74     ImaLinkFeRxUnusableSec = 57
        ImaLinkNeTxNumFailures = 0      ImaLinkNeRxNumFailures = 15
        ImaLinkFeTxNumFailures = 4      ImaLinkFeRxNumFailures = 3
ATM1/1 is up
        ImaLinkRowStatus = LinkRowStatusUnknown
        ImaLinkIfIndex   = 1            ImaLinkGroupIndex = 0
        ImaLinkState:
                NeTx = active
                NeRx = active
                FeTx = active
                FeRx = active
        ImaLinkFailureStatus:
                NeRx = noFailure
                FeRx = noFailure
        ImaLinkTxLid           = 1      ImaLinkRxLid           = 1
        ImaLinkRxTestPattern   = 65     ImaLinkTestProcStatus  = disabled
        ImaLinkRelDelay        = 0
IMA Link counters :
        ImaLinkImaViolations   = 1
        ImaLinkNeSevErroredSec = 40     ImaLinkFeSevErroredSec = 42
        ImaLinkNeUnavailSec    = 441389 ImaLinkFeUnAvailSec    = 38
        ImaLinkNeTxUnusableSec = 2      ImaLinkNeRxUnUsableSec = 441427
        ImaLinkFeTxUnusableSec = 99     ImaLinkFeRxUnusableSec = 99
        ImaLinkNeTxNumFailures = 0      ImaLinkNeRxNumFailures = 16
        ImaLinkFeTxNumFailures = 4      ImaLinkFeRxNumFailures = 4
```

Step 2 To see how SVCs and PVCs are set up, use the **show atm vc** command in privileged EXEC mode.

Example:

```
Router# show atm vc
VCD /                                      Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC    Kbps   Kbps   Cells  Sts
1/1        1            0    50   PVC    SNAP     UBR    1000              INAC
1/IMA3     2            0     5   PVC    SAAL     UBR    4000                UP
1/IMA3     3            0    16   PVC    ILMI     UBR    4000                UP
1/IMA3     first        1    13   PVC    MUX      VBR     640    320   80    UP
1/IMA3     4            0    34   SVC    SNAP     VBR-RT  768    768         UP
```

Troubleshooting Tips

To troubleshoot the ATM and IMA group configuration, enter the **ping** command, which checks host reachability and network connectivity. This command can confirm basic network connectivity on the AppleTalk, ISO CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks.

For IP, the **ping** command sends ICMP (Internet Control Message Protocol) Echo messages. If a station receives an ICMP Echo message, it sends an ICMP Echo Reply message back to the source.

The extended command mode of the **ping** command permits you to specify the supported IP header options so that the router can perform a more extensive range of test options. To enter **ping** extended command mode, enter **yes** at the "extended commands" prompt of the **ping** command.

For detailed information on using the **ping** and extended **ping** commands, see the *Cisco IOS Configuration Fundamentals Command Reference*.

If a **ping** command fails, check the following possible reasons for the connectivity problem:

- The interface is down, causing a "no ip route" error message.

- The PVC or SVC does not include proper mapping configured for the destination address, causing an "encapsulation failure" error. For more information about configuring encapsulation, see the section "Configuring IMA Groups, on page 65" earlier in this chapter and the **encapsulation aal5** command in the *Cisco IOS Asynchronous Transfer Mode Command Reference*.
- If there is a firmware problem, the **show controller atm**command shows whether an interface is able to transmit and receive cells. For sample output, see the earlier section "Verifying an ATM Interface Configured for IMA Operation, on page 61."

Tip Use the **ping** command when the network is functioning properly to see how the command works under normal conditions and so to compare the results when troubleshooting.

If a communication session is closing when it should not be, an end-to-end connection problem can be the cause. The **debug ip packet** command is useful for analyzing the messages traveling between the local and remote hosts. IP debugging information includes packets received, generated, and forwarded. Because the **debug ip packet** command generates a significant amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

Bandwidth Considerations

When planning IMA groups and payload bandwidth requirements, consider the overhead required for ATM cell headers, service-layer encapsulation such as RFC 1483, AAL5 encapsulation, and ICP cells. The tables below show approximate values for T1 and E1 IMA groups, respectively, with a frame length of 128, estimating ATM overhead at about 10 percent. The effective payload bandwidth varies according to packet size because the packets must be divided into an integer number of ATM cells leaving the last cell padded with filler bytes.

Note Control the bandwidth threshold to activate an IMA group by using the **ima active-links-minimum** command.

Table 1: T1 IMA AAL5 Payload Bandwidth with IMA Frame Size 128

Number of Links in the Group	Total Bandwidth	Payload Bandwidth
1	1.536	1.38
2	3.072	2.76
3	4.608	4.14
4	6.144	5.52
5	7.68	6.91
6	9.216	8.28
7	10.752	9.66

Number of Links in the Group	Total Bandwidth	Payload Bandwidth
8	12.288	11.04

Table 2: E1 IMA AAL5 Payload Bandwidth with IMA Frame Size 128

Number of Links in the Group	Total Bandwidth	Payload Bandwidth
1	1.92	1.74
2	3.84	3.47
3	5.76	5.21
4	7.68	6.95
5	9.60	8.69
6	11.52	10.43
7	13.44	12.17
8	15.36	13.90

Related Documents

For information about the physical characteristics of the ATM T1/E1 IMA network modules or port adapters, or for instructions on how to install the network or modem modules or port adapters, either see the installation guidelines that came with your network module or port adapter or view the up-to-date information on Cisco.com .

Configuring ATM E.164 Auto Conversion

E.164 is an International Telecommunications Union Telecommunication Standardization Sector (ITU-T) specification for the ISDN international telephone numbering plan, which has traditionally only been used in telephone networks. The ATM Forum has defined three different 20-byte ATM End System Address (AESA) formats, along with the native E.164 format, for use in ATM networks. One of these 20-byte formats is the embedded E.164 AESA (E164_AESA) format.

With ATM E.164 auto conversion enabled, networks that operate based on ATM addressing formats can internetwork with networks based on E.164 addressing formats. The conversion requires components from addressing, routing, and signaling to perform properly.

For more information about E.164 and ATM address formats, see ATM Forum UNI 3.0, 3.1, and 4.0, and ITU E.164. The table below lists the ATM and E.164 address formats supported by ATM E.164 auto conversion.

Table 3: ATM and E1.64 Address Formats

Address Type	Example
Native E.164 A minimum of 7 and maximum of 15 ASCII-encoded decimal numbers.	1-800-555-1212
E164_AESA E.164 ATM End System Address is an ATM address that contains an embedded E.164 number. Format |AFI | E164 | HO-DSP | ESI | SEL| AFI = 45	45.000018005551212F00000000.112233445566.00
E164_ZDSP E.164 Zero Domain Specific Part is an ATM address that contains all zeros in the Domain Specific Part of the address. Format |AFI | E164 | HO-DSP | ESI | SEL| AFI = 45 The remaining bytes in HO-DSP, ESI, and SEL are 0.	45.000018005551212F00000000.000000000000.00

When ATM E.164 auto conversion is enabled, a Cisco router sets up ATM SVC connections based on E.164 addresses. The router uses ATM E164_AESA addresses to set up E.164 calls in a way similar to using ATM AESA addresses to set up ATM SVCs. The ATM AESA address on an interface and the ATM AESA address of a static map must be in E164_AESA format.

Use the **show interfaces atm** command to verify that ATM E.164 auto conversion is running.

For an example of configuring ATM E.164 auto conversion, refer to the section "Example Configuring ATM E.164 Auto Conversion, on page 119" at the end of this chapter.

To configure ATM E.164 auto conversion, you must configure the ATM interface using E164_AESA or E164_ZDSP format. To enable E.164 auto conversion, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* /**0**
   -
   -
   - Router(config)# **interface atm** *slot* / *port-adapter* /**0**
2. Router(config-if)# **ip address** *ip-address mask*
3. Router(config-if)# **pvc 0/5 qsaal**
4. Router(config-if-atm-vc)# **exit**
5. Router(config-if)# **atm nsap-address** *nsap-address*
6. Router(config-if)# **atm e164 auto-conversion**
7. Router(config-if)# **svc** [*name*] **nsap** *address*
8. Router(config-if-atm-vc)# **protocol ip** *protocol-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* /**0** • • • Router(config)# **interface atm** *slot* / *port-adapter* /**0** **Example:** `Router(config)#` **interface atm** *number*	Specifies the ATM interface using the appropriate format of the **interface atm** command.[18]
Step 2	Router(config-if)# **ip address** *ip-address mask*	If IP routing is enabled on the system, optionally assigns a source IP address and subnet mask to the interface.
Step 3	Router(config-if)# **pvc 0/5 qsaal**	Configures the signaling PVC for the ATM main interface that uses SVCs.
Step 4	Router(config-if-atm-vc)# **exit**	Returns to interface configuration mode.
Step 5	Router(config-if)# **atm nsap-address** *nsap-address*	Sets the AESA address for the ATM interface using E164_AESA or E164_ZDSP address format.
Step 6	Router(config-if)# **atm e164 auto-conversion**	Enables E.164 auto conversion on the interface.

	Command or Action	Purpose
Step 7	Router(config-if)# **svc** [*name*] **nsap** *address*	Specifies the destination NSAP address using E164_AESA or E164_ZDSP address format.
Step 8	Router(config-if-atm-vc)# **protocol ip** *protocol-address*	Specifies the destination IP address of the SVC.

18 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Configuring Circuit Emulation Services

For overview information and configuration tasks for Circuit Emulation Services (CES) for ATM, see the following sections:

CES Overview

Circuit emulation service internetworking function (CES-IWF) is a service based on ATM Forum standards that allows communications to occur between CBR or AAL1 CES and ATM UNI interfaces; that is, between non-ATM telephony devices (such as classic PBXs or TDMs) and ATM devices (such as Cisco 3600 or 7200 series routers). Thus, a Cisco 3600 series router equipped with an OC-3/STM-1 ATM Circuit Emulation Service network module or a Cisco 7200 series router equipped with an ATM-CES port adapter offers a migration path from classic T1/E1 CBR data communications services to emulated CES T1/E1 unstructured (clear channel) services or structured (N x 64) services in an ATM network.

The figure below shows a simplified representation of CES-IWF functions in an ATM network.

Figure 5: Typical CES-IWF Operations in an ATM Network

CES allows you to interconnect existing T1 or E1 interfaces and other kinds of constant bit rate (CBR) equipment. CES includes such features as PBX interconnect, consolidated voice and data traffic, and video conferencing.

With circuit emulation, data received from an external device at the edge of an ATM network is converted to ATM cells, sent through the network, reassembled into a bit stream, and passed out of the ATM network to its destination. T1/E1 circuit emulation does not interpret the contents of the data stream. All the bits flowing into the input edge port of the ATM network are reproduced at one corresponding output edge port.

An emulated circuit is carried across the ATM network on a PVC, which is configured through the network management system or the router command line interface (CLI).

The target application of the OC-3/STM-1 ATM Circuit Emulation Service network module and the ATM-CES port adapter is access to a broadband public or private ATM network where multiservice consolidation of voice, video, and data traffic over a single ATM link is a requirement.

Configuring CES on the CES Network Module

To configure CES on the OC-3/STM-1 ATM Circuit Emulation Service network module, familiarize yourself with the restrictions in the first of the following sections and perform the tasks in the second, third, and fourth sections. Each task is identified as required or optional.

Note The configuration tasks in these sections are supported only on the OC-3/STM-1 ATM Circuit Emulation Service network module.

For an example of configuring CES on an OC-3/STM-1 ATM Circuit Emulation Service network module, see the section "Example Configuring CES on a CES Network Module, on page 120" at the end of this chapter.

Restrictions for th ATM CES Network Module

The OC-3/STM-1 ATM CES network module can be configured with the following restrictions:

- The OC-3/STM-1 ATM CES network module requires Cisco IOS Release 12.1(2)T or later.
- On-hook detection is not supported.
- If you configure an ABR VC, either in a vc-class or in vc mode, the minimum guaranteed cell rate (MCR) value you enter is ignored, and an MCR of 0 is used, although this is not apparent from the configuration. Additionally, ABR PCR values are configurable in a range from 0 to line rate. However, the MCR is honored. Currently, the OC-3/STM-1 ATM CES network module rounds the configured value down to one of the following values:
  - 64 Kbps
  - 384 K
  - 768 K
  - 1,534 K
  - 2 M
  - 4 M
  - 10 M
  - 16 M
  - 25.6 M
  - 44 M
  - 75 M
  - 100 M
  - 125 M
  - 149 M

- When you configure a UBR+ VC, the Cisco CLI requires that you specify a peak cell rate (PCR). Because of a hardware limitation, any value you enter is ignored by the OC-3/STM-1 ATM CES network module and a value of 155 Mbits per second is used.
- The OC-3/STM-1 ATM CES network module does not allow configuring interfaces and subinterfaces by using the **traffic-shape** parameter. That is because the OC-3/STM-1 ATM CES network module supports traffic shaping through native ATM means by making a traffic class for UBR, UBR+, ABR, VBR-rt, VBR-ntr, and CBR.

Configuring the ATM Interface

To configure the ATM interface on the OC-3/STM-1 ATM Circuit Emulation Service network module, perform the tasks in the following sections:

- Configuring PVCs for CES Operation, on page 81
- Configuring SVCs for CES Operation, on page 82

This section does not explain all possible ATM interface configuration options. For more information, see the sections "Configuring PVCs, on page 2" and "Configuring SVCs, on page 13" earlier in this chapter.

Configuring PVCs for CES Operation

To use a permanent virtual circuit (PVC), you must configure the PVC into both the router and the ATM switch. A PVC remains active until it is removed from either configuration. To configure the ATM interface with PVCs, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot* / *port*
2. Router(config-if)# **pvc** [*name*] *vpi* / *vci* [**ces**]
3. Router(config-if-ces-vc)# ces-cdv *time*
4. Router(config-if-ces-vc)# **exit**
5. Router(config-if)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot* / *port*	Selects the ATM interface to be configured.
Step 2	Router(config-if)# **pvc** [*name*] *vpi* / *vci* [**ces**]	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers, and enters interface-ATM-VC configuration mode. The **ces** keyword configures CES encapsulation, which is equivalent to creating a CBR class of service.
Step 3	Router(config-if-ces-vc)# ces-cdv *time*	Configures the cell delay variation. The *time* argument specifies the maximum tolerable cell arrival jitter with a range of 1 to 65535 microseconds.

	Command or Action	Purpose
Step 4	Router(config-if-ces-vc)# **exit**	Exits back to interface configuration mode.
Step 5	Router(config-if)# **exit**	Returns to global configuration mode.

Configuring SVCs for CES Operation

ATM switched virtual circuit (SVC) services are created and released dynamically, providing user bandwidth on demand. This service requires a signaling protocol between the router and the switch. To configure the ATM interface with SVCs, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot* / *port*
2. Router(config-if)# **pvc** name vpi/ *vci* [**qsaal** | **ilmi**]
3. Router(config-if-atm-vc)# **exit**
4. Router(config-if)# **svc** [*name*] **nsap** *address* **ces**
5. Router(config-if-atm-vc)# ces-cdv *time*
6. Router(config-if-atm-vc)# atm esi-address *esi* **.** *selector*
7. Router(config-if-atm-vc)# **exit**
8. Router(config-if)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot* / *port*	Selects the ATM interface to be configured.
Step 2	Router(config-if)# **pvc** name vpi/ *vci* [**qsaal** | **ilmi**]	Configures a new ATM PVC for signaling. One dedicated PVC is required between the router and the ATM switch, over which all SVC call establishment and call termination requests flow. Assign a name (optional) and VPI/VCI numbers. Specify **qsaal** to configure a signaling PVC. Specify **ilmi** to configure a PVC for communication with the Integrated Local Management Interface (ILMI). Enters interface-ATM-VC configuration mode.
Step 3	Router(config-if-atm-vc)# **exit**	Exits back to interface configuration mode.
Step 4	Router(config-if)# **svc** [*name*] **nsap** *address* **ces** **Example:**	Configures the active SVC and the ATM network service access point (NSAP) address. A passive SVC can be configured to only receive calls. The SVC name is required for this command. Enters interface-ATM-VC configuration mode.

	Command or Action	Purpose

	Example:
	
	Example:
	`Router(`
	`config-if`
	`)#` **svc** `[`*name*`]` **ces**	

Step 5	Router(config-if-atm-vc)# ces-cdv *time*	Configures the cell delay variation. The *time* argument specifies the maximum tolerable cell arrival jitter with a range of 1 to 65535 microseconds.
Step 6	Router(config-if-atm-vc)# atm esi-address *esi* **.** *selector*	Configures the endstation ID (ESI) and selector fields. This command is effective only if the switch is capable of delivering the NSAP address prefix to the router via ILMI and the router is configured with a PVC for communication with the switch via ILMI.
Step 7	Router(config-if-atm-vc)# **exit**	Exits back to interface configuration mode.
Step 8	Router(config-if)# **exit**	Returns to global configuration mode.

Configuring the T1 E1 Controller

The T1/E1 controller on the OC-3/STM-1 ATM Circuit Emulation Service network module provides T1 or E1 connectivity to PBXs or to a central office (CO). To configure the T1 or E1 controller on the OC-3/STM-1 ATM Circuit Emulation Service network module, perform the tasks in the following section. One of the first two tasks is required; the third task is optional:

For information about configuring the CES clock or echo cancellation, see the Cisco IOS Voice, Video, and Fax Configuration Guide .

For more information about configuring the T1/E1 interface on the OC-3/STM-1 ATM Circuit Emulation Service network module, see the Configuring 1- and 2-Port T1/E1 Multiflex Voice/WAN Interface Cards on Cisco 2600 and 3600 Series Routers Cisco IOS Release 12.0(5)XK online document.

Configuring Unstructured Circuit Emulation Service

This circuit consumes the entire bandwidth of the port, which is provisioned manually at the time you set up the unstructured circuit and remains dedicated to that port, whether that port is actively transmitting data or not.

A CES module converts non-ATM telephony traffic into ATM cells for propagation through an ATM network. The ATM cell stream is directed to an outgoing ATM port or non-ATM telephony port.

To configure the T1/E1 port for unstructured CES, follow this procedure starting in global configuration mode:

SUMMARY STEPS

1. Router(config)# **controller** {**T1** | **E1**} *slot* / *port*
2. Router(config-controller)# **ces-clock adaptive** | **srts** | **synchronous**
3. Router(config-controller)# **tdm-group** *tdm-group-no* **unstructured**
4. Router(config-controller)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller** {**T1** | **E1**} *slot* / *port*	Enters controller configuration mode for the T1 or E1 controller at the specified *slot* / *port*location. The prompt changes again to show that you are in controller configuration mode.
Step 2	Router(config-controller)# **ces-clock adaptive** | **srts** | **synchronous**	Selects the clock method. The default is synchronous.
Step 3	Router(config-controller)# **tdm-group** *tdm-group-no* **unstructured**	Configures a TDM channel group for the T1 interface.
Step 4	Router(config-controller)# **exit**	Returns to global configuration mode.

Configuring Structured Circuit Emulation Service

Structured CES differs from unstructured CES services in that the structured services allow you to allocate the bandwidth in a highly flexible and efficient manner. With the structured services, you use only the bandwidth actually required to support the active structured circuit(s) that you configure.

To configure the T1/E1 port for structured CES, follow this procedure starting in global configuration mode:

SUMMARY STEPS

1. Router(config)# **controller** {**T1** | **E1**} *slot* / *port*
2. Router(config-controller)# **clock source** {**line | internal}**
3. Do one of the following:
    - Router (config -controller)# **framing sf**| **esf**
    -
    -
    - Router (config -controller)# **framing crc4 no-crc4**} [**australia**
4. Router (config -controller)# **linecode b8zs**| **ami**| **hdb3**
5. Router(config-controller)# **ces-clock synchronous**
6. Router(config-controller)# **tdm-group** *tdm-group-no* **unstructured**
7. Router(config-controller)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller** {**T1** | **E1**} *slot* / *port*	Enters controller configuration mode for the T1 or E1 controller at the specified *slot* / *port*location. The prompt changes again to show that you are in controller configuration mode.
Step 2	Router(config-controller)# **clock source** {**line** | **internal**} **Example:**	Specifies which end of the circuit provides clocking for the T1 or E1 interface. The clock source can be set to use internal clocking for most applications.
Step 3	Do one of the following: • Router (config -controller)# **framing sf**| **esf** • • • Router (config -controller)# **framing crc4 no-crc4**} [**australia** **Example:**	Sets the framing to SuperFrame (SF) or Extended SuperFrame (ESF) format, according to service provider requirements. Sets the framing to cyclic redundancy check 4 (CRC4) or no CRC4, according to service provider requirements. The **australia** optional keyword specifies Australian Layer 1 Homologation for E1 framing.
Step 4	Router (config -controller)# **linecode b8zs**| **ami**| **hdb3** **Example:**	Sets the line encoding according to your service provider's instructions. Bipolar-8 zero substitution (B8ZS), available only for T1 lines, encodes a sequence of eight zeros in a unique binary sequence to detect line coding violations. Alternate mark inversion (AMI), available for T1 or E1 lines, represents zeros using a 01 for each bit cell, and ones are represented by 11 or 00, alternately, for each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. For E1, sets the line coding to either AMI or high-density bipolar 3 (HDB3), the default.
Step 5	Router(config-controller)# **ces-clock synchronous**	Specifies the type of clocking used for T1 interfaces using structured CES. Only synchronous clocking can be used with structured CES.
Step 6	Router(config-controller)# **tdm-group** *tdm-group-no* **unstructured**	Configures a time-division multiplexing (TDM) channel group for the T1 interface.
Step 7	Router(config-controller)# **exit**	Returns to global configuration mode.

Configuring Channel-Associated Signaling for Structured CES

Because the CES deck emulates constant bit rate services over ATM networks, it is capable of providing support for handling channel-associated signaling (CAS) information introduced into structured CES circuits by PBXs and time-division multiplexing (TDM) devices.

Note Only structured CES can support CAS.

The signaling supported depends on the WAN/voice interface card that is inserted in the CES deck. The signaling method depends on the connection that you are making:

- The receive and transmit (E&M) interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The wink and delay settings both specify confirming signals between the transmitting and receiving ends, whereas the immediate setting stipulates no special offhook/onhook signals.
- The FXO interface is for connection of a central office (CO) to a standard PBX interface where permitted by local regulations; the interface is often used for off-premises extensions.
- The FXS interface allows connection of basic telephone equipment and PBXs.

To configure the T1/E1 port for channel associated signaling, first perform the tasks in the Configuring Structured Circuit Emulation Service, on page 84 section, and then use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **controller** {**T1** | **E1**} *slot* / *port*
2. Router(config-controller)# **tdm-group** *tdm-group-no* **timeslots** *timeslot-list* **type** [**e&m** | **fxs** [**loop-start** | **ground-start**] **fxo**[**loop-start** | **ground-start**
3. Router(config-controller)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller** {**T1** | **E1**} *slot* / *port*	Enters controller configuration mode for the T1 or E1 controller at the specified slot/port location. The prompt changes again to show that you are in controller configuration mode.
Step 2	Router(config-controller)# **tdm-group** *tdm-group-no* **timeslots** *timeslot-list* **type** [**e&m** | **fxs** [**loop-start** | **ground-start**] **fxo**[**loop-start** | **ground-start**	Configures a TDM channel group for the T1 interface, including the signaling type. *tdm-group-no* is a value from 0 to 23 for T1 and from 0 to 30 for E1; it identifies the group. *timeslot-list* is a single number, numbers separated by commas, or a pair of numbers separated by a hyphen to indicate a range of time slots. The valid range is from 1 to 24 for T1. For E1, the range is from 1 to 31. **Note** The group numbers for controller groups must be unique. For example, a TDM group should not have the same ID number as a DS0 group or channel group.

	Command or Action	Purpose
Step 3	Router(config-controller)# **exit**	Returns to global configuration mode.

Activating the Connection

Once the ATM interface and T1 or E1 controllers are configured, activate the connection by using the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **connect** *connection-name* **atm** *slot* / *port* [*name of PVC/SVC* | *vpi* / *vci* **T1** *slot* / *port* TDM-group-number
2. Router(config-connect)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **connect** *connection-name* **atm** *slot* / *port* [*name of PVC/SVC* | *vpi* / *vci* **T1** *slot* / *port* TDM-group-number	Sets the connection to be activated.
Step 2	Router(config-connect)# **exit**	Exits config-connect mode. After exiting the config-connect mode, the connection is activated.

Verifying CES Configuration on the CES Network Module

To verify CES configuration on the OC-3/STM-1 ATM Circuit Emulation Service network module, use one or more of the following commands in EXEC mode:

Command	Purpose
`Router# show ces [ slot / port ]`	Displays detailed information about the CES connection
`Router# show ces [ slot / port ] clock-select`	Displays the setting of the network clock for the specified port.
`Router# show connection all`	Displays detailed information about the connections created by the **connect** command.
`Router# show controllers`	Displays all network modules and their interfaces.
`Router# show interfaces [ type slot/port ]`	Displays statistics for the interfaces configured on a router or access server. Verify that the first line of the display shows the interface with the correct slot and port number, and that the interface and line protocol are in the correct state, up or down.
`Router# show protocols`	Displays the protocols configured for the entire router and for individual interfaces.
`Router# show version`	Displays the router hardware configuration. Check that the list includes the new interface.

Configuring CES on the ATM-CES Port Adapter

To configure the T1/E1 interfaces on the ATM-CES port adapter for CES, perform the tasks in the following sections. One of the first two tasks is required:

Note The configuration tasks in these sections are supported only on the ATM-CES port adapter.

For an example of configuring CES on the ATM-CES port adapter, see the section "Example Configuring CES on an ATM-CES Port Adapter, on page 121" at the end of this chapter.

Configuring Unstructured Clear Channel CES Services

A circuit that you set up on a CBR port for unstructured service is always identified as "circuit 0" because only one such circuit can be established on any given CBR port. Such a circuit consumes the entire bandwidth of the port, which is provisioned manually at the time you set up the unstructured circuit and remains dedicated to that port whether that port is actively transmitting CBR data or not.

A CES module converts CBR traffic into ATM cells for propagation through an ATM network. The ATM cell stream is directed to an outgoing ATM port or CBR port. If the outgoing port is an ATM port on the same Cisco 7200 series router, the PVC is called a *hard PVC* . As a general rule when setting up a hard PVC, you must interconnect a CBR port and the ATM port in the same ATM-CES port adapter. Only hard PVCs are supported in the Cisco 7200 series router.

To configure the T1/E1 port on the ATM-CES port adapter for unstructured (clear channel) CES services, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface cbr** *slot* / *port*
2. Router(config-if)# **ces aal1 service** [**structured**| **unstructured**]
3. Router(config-if)# **ces aal1 clock** {**adaptive**| **srts**| **synchronous**}
4. Router(config-if)# **ces dsx1 clock source** {**loop-timed**| **network-derived**}
5. Router(config-if)# **ces circuit 0** [**circuit-name** *name*]
6. Router(config-if)# **ces pvc 0 interface atm** *slot* / *port* **vci** *number* **vpi** *number*
7. Router(config-if)# **no shutdown**
8. Router(config-if)# **no ces circuit 0 shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface cbr** *slot* / *port*	Specifies the ATM-CES port adapter interface.
Step 2	Router(config-if)# **ces aal1 service** [**structured**| **unstructured**]	Configures the port that is to perform unstructured CES services. The default is unstructured.
Step 3	Router(config-if)# **ces aal1 clock** {**adaptive**| **srts**| **synchronous**}	Optionally, selects the clock method. The default is synchronous.
Step 4	Router(config-if)# **ces dsx1 clock source** {**loop-timed**| **network-derived**}	If synchronous clocking is selected, configures the clock source.
Step 5	Router(config-if)# **ces circuit 0** [**circuit-name** *name*]	Specifies the circuit number for unstructured services and optionally specifies the logical name of the PVC. If you do not specify a circuit name, the default is CBRx/x:x.
Step 6	Router(config-if)# **ces pvc 0 interface atm** *slot* / *port* **vci** *number* **vpi** *number*	Defines the particular ATM destination port for the PVC.

	Command or Action	Purpose
Step 7	Router(config-if)# **no shutdown**	Changes the shutdown state to up and enables the ATM interface, thereby beginning the segmentation and reassembly (SAR) operation on the interface.
Step 8	Router(config-if)# **no ces circuit 0 shutdown**	Enables the PVC.

Configuring Structured N x 64 CES Services

Structured (N x 64 kbps) CES services differ from unstructured CES services in that the structured services allow you to allocate the bandwidth in a highly flexible and efficient manner. With the structured services, you use only the bandwidth actually required to support the active structured circuit that you configure.

For example, in configuring an ATM-CES port adapter for structured service, you can define multiple hard PVCs for any given ATM-CES port adapter's T1/E1 port. The ATM-CES port adapter provides up to 24 time slots per T1 port and up to 31 time slots per E1 for defining structured CES circuits. To see the bandwidth that is required on an ATM link for this particular circuit, use the **show ces circuit**command.

Note In the ATM-CES port adapter, any bits not available for structured CES services are used for framing and out-of-band control.

For simplicity in demonstrating configuration tasks for structured CES services, the procedures in this section are directed primarily at setting up a single CES circuit per T1/E1 port. However, these procedures outline the essential steps and command syntax that you would use if you were to set up multiple CES circuits on a T1/E1 port.

Structured CES services require network clock synchronization by means of the synchronous clocking mode. You must select the clock source and define its priority locally for each Cisco 7200 series router in your network. You do this by means of the **network-clock-select** command.

To configure the T1/E1 port on the ATM-CES port adapter for structured (N x 64 kbps) CES services without CAS, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface cbr** *slot* / *port*
2. Router(config-if)# **ces aal1 service** [**structured** | **unstructured**]
3. Router(config-if)# **ces aal1 clock** {**adaptive**| **srts** | **synchronous**}
4. Router(config-if)# **ces dsx1 clock source** {**loop-timed**| **network-derived**}
5. Do one of the following:
    - Router(config-if)# **ces dsx1 linecode** {**ami** | **b8zs**}
    - (for T1)
    -
    -
    -
6. Do one of the following:
    - Router(config-if)# **ces dsx1 framing** {**esf** | **sf**}
    - (for T1)
    -
    -
    -
7. Router(config-if)# **ces dsx1 lbo** *length*
8. Router(config-if)# **ces circuit** *circuit-number* [**circuit-name** *name*]
9. Router(config-if)# **ces circuit** *circuit-number* **timeslots** *range*
10. Router(config-if)# **ces circuit** *circuit-number* **cdv** *range*
11. Router(config-if)# **ces pvc** *circuit-number* **interface atm** *slot* / *port* **vpi** *number* **vci** *number*
12. Router(config-if)# **no shutdown**
13. Router(config-if)# **no ces circuit** *circuit-number* **shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface cbr** *slot* / *port*	Specifies the ATM-CES port adapter interface.
Step 2	Router(config-if)# **ces aal1 service** [**structured** | **unstructured**]	Configures the port to perform structured CES services. The default is unstructured.
Step 3	Router(config-if)# **ces aal1 clock** {**adaptive**| **srts** | **synchronous**}	Optionally, selects the clock method. The default is synchronous. Adaptive and SRTS are available only for unstructured mode.
Step 4	Router(config-if)# **ces dsx1 clock source** {**loop-timed**| **network-derived**}	If synchronous clocking is selected, configures the clock source.

	Command or Action	Purpose
Step 5	Do one of the following: • Router(config-if)# **ces dsx1 linecode** {**ami** | **b8zs**} • (for T1) • • • **Example:** `Router(config-if)#` **ces dsx1 linecode {ami** | **hdb3**} **Example:** `(for E1)`	Specifies the line code format used for the physical layer. The default is AMI.
Step 6	Do one of the following: • Router(config-if)# **ces dsx1 framing** {**esf** | **sf**} • (for T1) • • • **Example:** `Router(config-if)#` **ces dsx1 framing** {**e1_crc_mfCASlt** | **e1_crc_mf_lt** | **e1_lt** | **e1_mfCAS_lt**} **Example:** `(for E1)`	Specifies the framing format The default for T1 is ESF and for E1 is E1_LT.
Step 7	Router(config-if)# **ces dsx1 lbo** *length*	Optionally, specifies the line build out (cable length). Values are (in feet): 0_110, 110_220, 220_330, 330_440, 440_550, 550_660, 660_above, and square_pulse. The default is 0_110 feet.
Step 8	Router(config-if)# **ces circuit** *circuit-number* [**circuit-name** *name*]	Specifies the circuit number for structured services and optionally specifies the logical name of the PVC. For T1 structured service, the range is 1 through 24. For E1 structured service, the range is 1 through 31. If you do not specify a circuit name, the default is CBRx/x:x.

	Command or Action	Purpose
Step 9	Router(config-if)# **ces circuit** *circuit-number* **timeslots** *range*	Specifies the time slots to be used by the PVC. For T1, the range is 1 through 24. For E1 structured service, the range is 1 through 31. Use a hyphen to indicate a range (for example, 1-24). Use a comma to separate the time slot (for example, 1,3,5).
Step 10	Router(config-if)# **ces circuit** *circuit-number* **cdv** *range*	Optionally, configures the circuit cell delay variation. Range is 1 through 65535 milliseconds. The default range is 2000 milliseconds.
Step 11	Router(config-if)# **ces pvc** *circuit-number* **interface atm** *slot* / *port* **vpi** *number* **vci** *number*	Defines the particular ATM destination port for the PVC.
Step 12	Router(config-if)# **no shutdown**	Changes the shutdown state to up and enables the ATM interface, thereby beginning the segmentation and reassembly (SAR) operation on the interface.
Step 13	Router(config-if)# **no ces circuit** *circuit-number* **shutdown**	Enables the PVC.

What to Do Next

Note You need not specify individual circuit options on a separate command line. If you want, you can specify all the desired circuit options on the same command line, provided that you observe the following rules: (1) specify the DS0 time slots as the first option; (2) specify each desired option thereafter in strict alphabetic order; and (3) separate consecutive command line options with a space. You can display the options available for any structured CES circuit by typing the **ces circuit** *circuit-number* **?** command, which displays in alphabetic order all the options available for use in the command line.

Configuring Channel-Associated Signaling for Structured CES Services

Because the ATM-CES port adapter emulates constant bit rate services over ATM networks, it must be capable of providing support for handling channel-associated signaling (CAS) information introduced into structured CES circuits by PBXs and time-division multiplexing (TDM) devices. The **ces circuit cas**interface command provides this feature.

With respect to the CAS information carried in a CBR bit stream, an ATM-CES port adapter can be configured to operate as follows:

- Without the CAS feature enabled (the default state)

In this case, the ATM-CES port adapter does not sense the CAS information (carried as so-called "ABCD" bits in the CBR bit stream) and provides no support for CAS functions.

- With the CAS feature enabled, but without the (Cisco-proprietary) "on-hook detection" feature enabled

In this case, in addition to packaging incoming CBR data into ATM AAL1 cells in the usual manner for transport through the network, the ATM-CES port adapter in the ingress node senses the ABCD bit patterns in the incoming data, incorporates these patterns in the ATM cell stream, and propagates the cells to the next node in the network. The ATM cells are transported across the network from link to link until the egress node is reached.

At the egress node, the ATM-CES port adapter strips off the ABCD bit patterns carried by the ATM cells, reassembles the CAS ABCD bits and the user's CBR data into original form, and passes the frames out of the ATM network in the proper DS0 time slot.

All these processes occur transparently without user intervention.

- With both the CAS and on-hook detection features enabled

In this case, the CAS and on-hook detection features work together to enable an ingress node in an ATM network to monitor on-hook and off-hook conditions for a specified 1 x 64 structured CES circuit. As implied by the notation "1 x 64," the on-hook detection (or bandwidth-release) feature is supported only in a structured CES circuit that involves a single time slot at each end of the connection.

The time slot configured for the structured CES circuit at the ingress node (time slot 2) can be different from the DS0 time slot configured at the egress node (time slot 4). Only one such time slot can be configured at each end of the circuit when the on-hook detection feature is used.

When you invoke this feature, the ingress ATM-CES port adapter monitors the ABCD bits in the incoming CBR bit stream to detect on-hook and off-hook conditions in the circuit. In an "off-hook" condition, all the bandwidth provisioned for the specified CES circuit is used for transporting ATM AAL1 cells across the network from the ingress node to the egress node.

In an on-hook condition, the network periodically sends dummy ATM cells from the ingress node to the egress node to maintain the connection. However, these dummy cells consume only a fraction of the circuit's reserved bandwidth, leaving the rest of the bandwidth available for use by other AAL5 network traffic. This bandwidth-release feature enables the network to make more efficient use of its resources.

When the CAS feature is enabled for a CES circuit, the bandwidth of the DS0 channel is limited to 56 kbps for user data, because CAS functions consume 8 kbps of channel bandwidth for transporting the ABCD signaling bits. These signaling bits are passed transparently from the ingress node to the egress node as part of the ATM AAL1 cell stream.

In summary, when the optional CAS and on-hook detection features are enabled, the following conditions apply:

- The PVC provisioned for the CES circuit always exists.
- During an on-hook state, most of the bandwidth reserved for the CES circuit is not in use. (Dummy cells are sent from the ingress node to the egress node to maintain the connection.) Therefore, this bandwidth becomes available for use by other AAL5 network traffic, such as available bit rate (ABR) traffic.
- During an off-hook state, all the bandwidth reserved for the CES circuit is dedicated to that circuit.

To configure the T1/E1 port on the ATM-CES port adapter for channel-associated signaling, first use the commands in the section "Configuring Structured N x 64 CES Services, on page 90", and then use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface cbr** *slot* / *port*
2. Router(config-if)# **ces circuit** *circuit-number* **cas**
3. Router(config-if)# **ces dsx1 signalmode robbedbit**
4. Router(config-if)# **ces circuit** *circuit-number* **on-hook-detection** *hex-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface cbr** *slot* / *port*	Specifies the ATM-CES port adapter interface.
Step 2	Router(config-if)# **ces circuit** *circuit-number* **cas**	Enables channel-associated signaling.
Step 3	Router(config-if)# **ces dsx1 signalmode robbedbit**	(Optional) Enables the signal mode as robbed bit.
Step 4	Router(config-if)# **ces circuit** *circuit-number* **on-hook-detection** *hex-number*	(Optional) Enables on-hook detection.

Configuring Network Clock Source and Priorities

You can specify up to four network clock sources for a Cisco 7200 series router. The highest-priority active port in the chassis supplies the primary reference source to all other chassis interfaces that require network clock synchronization services. The fifth network clock source is always the local oscillator on the ATM-CES port adapter.

To direct a CBR port to use the network-derived clock, you must configure the CBR port with the **ces dsx1 clock source network-derived** interface command. For information on configuring the CBR port, refer to the section "Configuring Unstructured Clear Channel CES Services, on page 89" earlier in this chapter.

To verify the clock signal sources and priorities that you have established for your ATM-CES port adapter, use the **show network-clocks**privileged EXEC command.

Note The commands in this section are supported only on the ATM-CES port adapter.

For an example of configuring the network clock source and priority, see the section "Example Configuring Network Clock Source Priority, on page 122" at the end of this chapter.

To establish the sources and priorities of the requisite clocking signals for an ATM-CES port adapter in a Cisco 7200 series router, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **network-clock-select 1** {**atm** | **cbr**} *slot* / *port*
2. Router(config)# **network-clock-select 2** {**atm** | **cbr**} *slot* / *port*
3. Router(config)# **network-clock-select 3** {**atm** | **cbr**} *slot* / *port*
4. Router(config)# **network-clock-select 4** {**atm** | **cbr**} *slot* / *port*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **network-clock-select 1** {**atm** | **cbr**} *slot* / *port*	Establishes a priority 1 clock source.
Step 2	Router(config)# **network-clock-select 2** {**atm** | **cbr**} *slot* / *port*	Establishes a priority 2 clock source.
Step 3	Router(config)# **network-clock-select 3** {**atm** | **cbr**} *slot* / *port*	Establishes a priority 3 clock source.
Step 4	Router(config)# **network-clock-select 4** {**atm** | **cbr**} *slot* / *port*	Establishes a priority 4 clock source.

Configuring Virtual Path Shaping

The OC-3/STM-1 ATM Circuit Emulation Service Network Module and ATM-CES port adapter support multiplexing of one or more PVCs over a virtual path (VP) that is shaped at a constant bandwidth. To use this feature, you must configure a permanent virtual path (PVP) with a specific virtual path identifier (VPI). Any PVCs that are created subsequently with the same VPI are multiplexed onto this VP; the traffic parameters of individual PVCs are ignored.

The traffic shaping conforms to the peak rate that is specified when you create the VP. Any number of data PVCs can be multiplexed onto a VP.

Note In the case of local switching, you cannot configure VP with interworking.

For an example of virtual path shaping, see the section "Example Configuring Virtual Path Shaping, on page 122" at the end of this chapter.

To create a PVP, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **atm pvp** *vpi* [*peak-rate*]
2. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
3. Router(config-if)# **exit**
4. Router(@) show atm vp

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **atm pvp** *vpi* [*peak-rate*]	Creates a PVP and optionally specifies the peak rate. • The value of the *vpi* argument is the virtual path identifier to be associated with the PVP (valid values are in the range from 0 to 255 inclusive). The *peak-rate* argument is the maximum rate (in kbps) at which the PVP is allowed to transmit data. Valid values are in the range 84 kbps to line rate. The default peak rate is the line rate. • If you change the peak rate online, the ATM port will go down and then up. • If you create a PVP for performing the local switching of an L2 transport protocol or for the **xconnect** command configuration, the OAM PVCs are created only if the PVP is successfully created. • Range VCs are not supported in ATM PVP.
Step 2	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	(Optional) Creates a PVC with a VPI that matches the VPI specified in Step 1. • The **pvc** command is rejected if a nonmultiplexed PVC with the specified VPI value already exists. This could happen if you first create a PVC with a given VPI value, and then you subsequently enter this command. • When you create a PVP, two PVCs are created (with VCI 3 and 4) by default. These PVCs are created for VP end-to-end loopback and segment loopback OAM support.
Step 3	Router(config-if)# **exit**	Exits interface configuration mode.
Step 4	Router(@) show atm vp	Displays information about the PVP.

Configuring ATM Access over a Serial Interface

This section describes how to configure routers that use a serial interface for ATM access through an ATM data service unit (ADSU). The configuration tasks include the steps necessary to enable Asynchronous Transfer Mode-Data Exchange Interface (ATM-DXI) encapsulation, select a multiprotocol encapsulation method using ATM-DXI, and set up a PVC for the selected encapsulation.

In routers with a serial interface, an ADSU is required to provide the ATM interface to the network, convert outgoing packets into ATM cells, and reassemble incoming ATM cells into packets.

Any serial interface can be configured for multiprotocol encapsulation over ATM-DXI, as specified by RFC 1483. At the ADSU, the DXI header is stripped off, and the protocol data is segmented into cells for transport over the ATM network.

RFC 1483 describes two methods of transporting multiprotocol connectionless network interconnect traffic over an ATM network. One method allows multiplexing of multiple protocols over a single PVC. The other method uses different virtual circuits to carry different protocols. Cisco's implementation of RFC 1483 supports both methods and supports transport of Apollo Domain, AppleTalk, Banyan VINES, DECnet, IP, Novell IPX, ISO CLNS, and XNS traffic.

To configure ATM access over a serial interface, complete the tasks in the following sections. The first four tasks are required.

For an example of configuring ATM access over a serial interface, see the section "Example ATM Access over a Serial Interface, on page 122" at the end of this chapter.

Enabling the Serial Interface

The supported protocols are Apollo Domain, AppleTalk, Banyan VINES, DECnet, IP, Novell IPX, ISO CLNS, and XNS.

For information about the addressing requirements of a protocol, see the relevant protocol configuration chapter in the Cisco IOS IP Configuration Guide , the Cisco IOS AppleTalk and Novell IPX Configuration Guide, or the Cisco IOS Apollo Domain , Banyan VINES , DECnet , ISO CLNS , and XNS Configuration Guide .

To configure the serial interface for ATM access, enable the serial interface by using the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface serial** *number*
2. Do one of the following:
   - Router(config-if)# **appletalk address** *network* **.** *node*
   -
   - Router(config-if)# **ip address** *address mask*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface serial** *number*	Enables the serial interface.
Step 2	Do one of the following: • Router(config-if)# **appletalk address** *network* **.** *node* • • Router(config-if)# **ip address** *address mask* **Example:** **Example:** `Router(config-if)#` **ipx network** *number*	For each protocol to be carried, assigns a protocol address to the interface. (The commands shown are a partial list for the supported protocols.)

Enabling ATM-DXI Encapsulation

To enable ATM-DXI encapsulation on a serial or High-Speed Serial Interface (HSSI), use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **encapsulation atm-dxi**	Enables ATM-DXI encapsulation.

Setting Up the ATM-DXI PVC

An ATM-DXI PVC can be defined to carry one or more protocols as described by RFC 1483, or multiple protocols as described by RFC 1490.

The multiplex (MUX) option defines the PVC to carry one protocol only; each protocol must be carried over a different PVC. The Subnetwork Access Protocol (SNAP) option is LLC/SNAP multiprotocol encapsulation, compatible with RFC 1483; SNAP is the current default option. The network layer protocol identification (NLPID) option is multiprotocol encapsulation, compatible with RFC 1490; this option is provided for backward compatibility with the default setting in earlier versions in the Cisco IOS software.

Note The default encapsulation was NLPID in software earlier than Release 10.3. Beginning in that release, the default encapsulation is SNAP. Select the **nlpid** keyword now if you had previously selected the default.

To set up the ATM-DXI PVC and select an encapsulation method, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **dxi pvc** *vpi vci* [**snap** | **nlpid** | **mux**]	Defines the ATM-DXI PVC and the encapsulation method.

Mapping Protocol Addresses to the ATM-DXI PVC

This section describes how to map protocol addresses to the VCI and the VPI of a PVC that can carry multiprotocol traffic. The protocol addresses belong to the host at the other end of the link.

The supported protocols are Apollo Domain, AppleTalk, Banyan VINES, DECnet, IP, Novell IPX, ISO CLNS, and XNS.

For an example of configuring a serial interface for ATM, see the section "Example ATM Access over a Serial Interface, on page 122" later in this chapter.

To map a protocol address to an ATM-DXI PVC, use the following command in interface configuration mode (repeat this task for each protocol to be carried on the PVC):

Command	Purpose
Router(config-if)# **dxi map** *protocol protocol-address vpi vci* [**broadcast**]	Maps a protocol address to the ATM-DXI PVC's VPI and VCI.

Monitoring and Maintaining the ATM-DXI Serial Interface

After configuring the serial interface for ATM, you can display the status of the interface, the ATM-DXI PVC, or the ATM-DXI map. To display interface, PVC, or map information, use the following commands in EXEC mode:

Command	Purpose
Router# **show interfaces atm** [*slot* / *port*]	Displays the serial ATM interface status.
Router# **show dxi pvc**	Displays the ATM-DXI PVC information.
Router# **show dxi map**	Displays the ATM-DXI map information.

Troubleshooting the ATM Interface

The **atm oam flush** command is a diagnostic tool that drops all OAM cells that are received on an ATM interface. To drop all incoming OAM cells on an ATM interface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
    - Router(config)# **interface atm** *slot* **/0**
    -
    -
    - Router(config)# **interface atm** *slot* / *port-adapter* **/0**
2. Router(config-if)# **atm oam flush**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0** • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0** **Example:** **Example:** **Example:** `Router(config)#` **interface atm** *number*	Specifies the ATM interface using the appropriate format of the **interface atm** command.[19]
Step 2	Router(config-if)# **atm oam flush**	Specifies that incoming OAM cells be dropped on the ATM interface.

19 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Monitoring and Maintaining the ATM Interface

After configuring an ATM interface, you can display its status. You can also display the current state of the ATM network and connected virtual circuits. To show current virtual circuits and traffic information, use the following commands in EXEC mode:

Command	Purpose
`Router#` **show arp**	Displays entries in the ARP table.
`Router#` **show atm class-links** {*vpi* / *vci* | *name*}	Displays PVC and SVC parameter configurations and where the parameter values are inherited from.
`Router#` **show atm interface atm** *slot* **/0** `Router#` **show atm interface atm** *slot* / *port-adapter* **/0** `Router#` **show atm interface atm** *number*	Displays ATM-specific information about the ATM interface using the appropriate format of the **show atm interface atm** command.[20]
`Router#` **show atm map**	Displays the list of all configured ATM static maps to remote hosts on an ATM network.
`Router#` **show atm pvc** [*vpi* / *vci* | *name* | **interface atm** *interface_number*]	Displays all active ATM PVCs and traffic information.
`Router#` **show atm svc** [*vpi* / *vci* | *name* | **interface atm** *interface_number*]	Displays all active ATM SVCs and traffic information.
`Router#` **show atm traffic**	Displays global traffic information to and from all ATM networks connected to the router, OAM statistics, and a list of counters of all ATM traffic on this router.
`Router#` **show atm vc** [*vcd-number* | [**range** *lower-limit-vcd upper-limit-vcd*] [**interface ATM** *interface-number*] [**detail** [**prefix** {**vpi/vci** | **vcd** | **interface** | **vc_name**}]] [*connection-name*] | **signalling** [**freed-svcs** | [**cast-type**{**p2mp** | **p2p**}] [**detail**] [**interface ATM** *interface-number*]] | **summary ATM** *interface-number*]	Displays all active ATM virtual circuits (PVCs and SVCs) and traffic information. **Note** The SVCs and the **signalling** keyword are not supported on the Cisco ASR 1000 series routers.
`Router#` **show controllers atm** [*slot* **/ima** *group-number*]	Displays information about current settings and performance at the physical level.
	Displays general or detailed information about IMA groups and the links in those groups.

Command	Purpose
Router# **show ima interface atm** [*slot*]**/ima** [*group-number*] [**detail**]	
Router# **show interfaces atm** Router# **show interfaces atm** *slot* **/0** Router# **show interfaces atm** *slot* / *port-adapter* **/0**	Displays statistics for the ATM interface using the appropriate format of the **show interfaces atm** command.
Router# **show network-clocks**	Displays the clock signal sources and priorities that you established on the router.
Router# **show sscop**	Displays SSCOP details for the ATM interface.

20 To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

ATM Configuration Examples

The examples in the following sections illustrate how to configure ATM for the features described in this chapter. The examples below are presented in the same order as the corresponding configuration task sections presented earlier in this chapter:

Example Creating a PVC

The following example shows how to create a PVC on an ATM main interface with AAL5/MUX encapsulation configured and a VBR-NRT QOS specified. For further information, refer to the sections "Creating a PVC, on page 3" and "Configuring PVC Traffic Parameters, on page 4" earlier in this chapter.

```
interface 2/0
 pvc cisco 1/40
 encapsulation aal5mux ip
 vbr-nrt 100000 50000 20
 exit
```

Examples PVC with AAL5 and LLC SNAP Encapsulation

The following example shows how to create a PVC 0/50 on ATM interface 3/0. It uses the global default LLC/SNAP encapsulation over AAL5. The interface is at IP address 10.1.1.1 with 10.1.1.5 at the other end of the connection. For further information, refer to the sections "Creating a PVC, on page 3" and "Mapping a Protocol Address to a PVC, on page 3" earlier in this chapter.

```
interface atm 3/0
 ip address 10.1.1.1 255.255.255.0
 pvc 0/50
 protocol ip 10.1.1.5 broadcast
```

```
 exit
!
 ip route-cache cbus
```

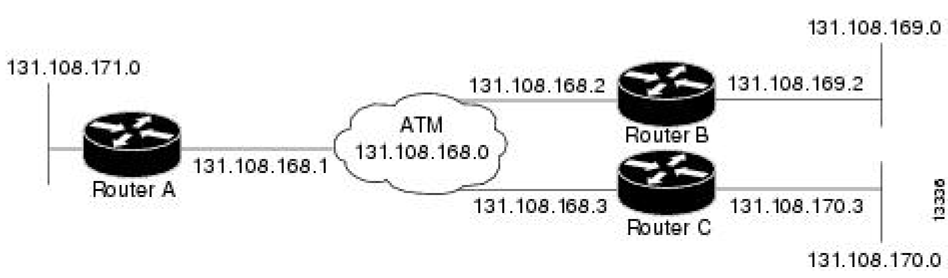
The following example is a typical ATM configuration for a PVC:

```
interface atm 4/0
 ip address 172.21.168.112 255.255.255.0
 atm maxvc 512
 pvc 1/51
 protocol ip 172.21.168.110
 exit
!
 pvc 2/52
 protocol decnet 10.1 broadcast
 exit
!
 pvc 3/53
 protocol clns 47.004.001.0000.0c00.6e26.00 broadcast
 exit
!
 decnet cost 1
 clns router iso-igrp comet
 exit
!
router iso-igrp comet
 net 47.0004.0001.0000.0c00.6666.00
 exit
!
router igrp 109
 network 172.21.0.0
 exit
!
ip domain-name CISCO.COM
```

Example VCs in a Fully Meshed Network

The figure below illustrates a fully meshed network. The configurations for routers A, B, and C follow the figure. In this example, the routers are configured to use PVCs. Fully meshed indicates that any workstation can communicate with any other workstation. Note that the two **protocol** statements configured in router A identify the ATM addresses of routers B and C. The two **protocol**statements in router B identify the ATM addresses of routers A and C. The two **protocol** statements in router C identify the ATM addresses of routers A and B. For further information, refer to the sections "Creating a PVC, on page 3" and "Mapping a Protocol Address to a PVC, on page 3" earlier in this chapter.

Figure 6: Fully Meshed ATM Configuration Example



Router A

```
ip routing
!
```

```
interface atm 4/0
 ip address 172.108.168.1 255.255.255.0
 pvc 0/32
 protocol ip 172.108.168.2 broadcast
 exit
!
 pvc 0/33
 protocol ip 172.108.168.3 broadcast
 exit
```

Router B

```
ip routing
!
interface atm 2/0
 ip address 172.108.168.2 255.255.255.0
 pvc test-b-1 0/32
 protocol ip 172.108.168.1 broadcast
 exit
!
 pvc test-b-2 0/34
 protocol ip 172.108.168.3 broadcast
 exit
```

Router C

```
ip routing
!
interface atm 4/0
 ip address 172.108.168.3 255.255.255.0
 pvc 0/33
 protocol ip 172.108.168.1 broadcast
 exit
!
 pvc 0/34
 protocol ip 172.108.168.2 broadcast
 exit
```

Example Configuring an ABR PVC

The following example shows a typical ABR PVC configuration for the ATM-CES port adapter on a Cisco 7200 series router. In this example, the default peak cell rate and minimum cell rate is used (default PCR is the line rate and MCR is 0), and the ABR rate increase and decrease factor is set to 32. For further information, refer to the section "Configuring PVC Traffic Parameters, on page 4" earlier in this chapter.

```
interface atm 4/0
 ip address 10.1.1.1 255.255.255.0
 pvc 0/34
 atm abr rate-factor 32 32
 no shutdown
 exit
```

Example Configuring PVC Discovery

The following example shows how to enable PVC Discovery on an ATM main interface 2/0. The keyword **subinterface** is used so that all discovered PVCs with a VPI value of 1 will be assigned to the subinterface

2/0.1. For further information, refer to the section "Configuring PVC Discovery, on page 5" earlier in this chapter.

```
interface atm 2/0
 pvc RouterA 0/16 ilmi
 exit
 atm ilmi-pvc-discovery subinterface
 exit
!
interface atm 2/0.1 multipoint
 ip address 172.21.51.5 255.255.255.0
```

Example Enabling Inverse ARP

The following example shows how to enable Inverse ARP on an ATM interface and specifies an Inverse ARP time period of 10 minutes. For further information, refer to the section "Enabling Inverse ARP, on page 8" earlier in this chapter.

```
interface atm 2/0
 pvc 1/32
 inarp 10
 exit
```

Example Configuring Loopback Cells

The following example shows how to enable OAM management on an ATM PVC. The PVC is assigned the name routerA and the VPI and VCI are 0 and 32, respectively. OAM management is enabled with a frequency of 3 seconds between OAM cell transmissions. For further information, refer to the section "Configuring Loopback Cells to Verify Connectivity, on page 9" earlier in this chapter.

```
interface atm 2/0
 pvc routerA 0/32
 oam-pvc manage 3
 oam retry 5 5 10
```

Example Configuring PVC Trap Support

The following example shows how to configure PVC trap support on your Cisco router:

```
!For PVC trap support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.69.61.90 public

Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.21.0.0
!
!Enable PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
!
! Now if PVC 0/1 goes down, host 171.69.61.90 will receive traps.
```

For further information, refer to the "Configuring PVC Trap Support, on page 11" section earlier in this chapter.

Example Configuring Communication with the ILMI

The following example shows how to configure the ILMI protocol on an ATM main interface. For further information, refer to the section "Configuring Communication with the ILMI, on page 14" earlier in this chapter.

```
interface 2/0
 pvc cisco 0/16 ilmi
 exit
```

Example SVCs in a Fully Meshed Network

The following example is also a configuration for the fully meshed network, but this example uses SVCs. PVC 0/5 is the signaling PVC.

Note Configuring explicit ATM NSAP addresses on the routers in this example also requires configuring static call routing on the ATM switch in order to route the calls properly. For more information on how to configure static call routing, refer to your switch documentation.

For further information, see the following sections earlier in this chapter:

- Configuring the PVC That Performs SVC Call Setup, on page 15
- Configuring the NSAP Address, on page 16
- Creating an SVC, on page 17

Router A

```
interface atm 4/0
 ip address 172.16.168.1 255.255.255.0
 atm nsap-address AB.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
 atm maxvc 1024
 pvc 0/5 qsaal
 exit
!
 svc svc-1 nsap BC.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.13
 protocol ip 172.16.168.2
 exit
!
 svc svc-2 nsap CA.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.12
 protocol ip 172.108.168.3
 exit
```

Router B

```
interface atm 2/0
 ip address 172.16.168.2 255.255.255.0
 atm nsap-address BC.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.13
 atm maxvc 1024
 pvc 0/5 qsaal
 exit
!
 svc svc-1 nsap AB.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
 protocol ip 172.16.168.1
 exit
```

```
!
 svc svc-2 nsap CA.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.12
 protocol ip 172.16.168.3
 exit
```

Router C

```
interface atm 4/0
ip address 172.16.168.3 255.255.255.0
atm nsap-address CA.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.12
atm maxvc 1024
pvc 0/5 qsaal
exit
!
svc nsap AB.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
protocol ip 172.16.168.1
exit
!
svc nsap BC.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.13
protocol ip 172.16.168.2
exit
```

Example ATM ESI Address

The following example shows how to set up the ILMI PVC and how to assign the ESI and selector field values on a Cisco 7500 series router. For further information, refer to the section "Configuring the ESI and Selector Fields, on page 16" earlier in this chapter.

```
interface atm 4/0
 pvc 0/16 ilmi
 atm esi-address 345678901234.12
```

Example ATM NSAP Address

The following example shows how to assign NSAP address AB.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12 to ATM interface 4/0. For further information, refer to the section "Configuring the Complete NSAP Address, on page 17" earlier in this chapter.

```
interface atm 4/0
 atm nsap-address AB.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
```

You can display the ATM address for the interface by executing the **show interface atm**command.

Example SVCs with Multipoint Signaling

The following example shows how to configure an ATM interface for SVCs using multipoint signaling. For further information, refer to the section "Configuring Point-to-Multipoint Signaling, on page 19" earlier in this chapter.

```
interface atm 2/0
 ip address 10.4.4.6 255.255.255.0
 pvc 0/5 qsaal
 exit
!
 pvc 0/16 ilmi
 exit
!
 atm esi-address 3456.7890.1234.12
```

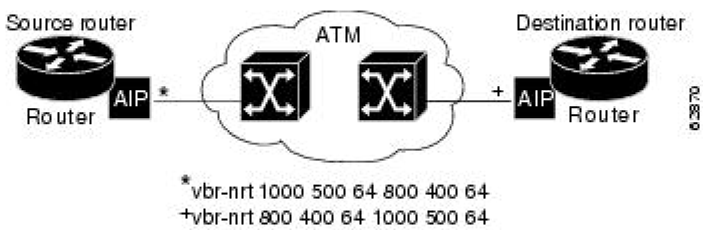
```
!
 svc mcast-1 nsap cd.cdef.01.234566.890a.bcde.f012.3456.7890.1234.12 broadcast
 protocol ip 10.4.4.4 broadcast
 exit
!
 svc mcast-2 nsap 31.3233.34.352637.3839.3031.3233.3435.3637.3839.30 broadcast
 protocol ip 10.4.4.7 broadcast
 exit
!
 atm multipoint-signalling
 atm maxvc 1024
```

Example Configuring SVC Traffic Parameters

The figure below illustrates a source and destination router implementing traffic settings that correspond end-to-end. The output values for the source router correspond to the input values for the destination router. The following example shows how to specify VBR-NRT traffic parameters on the source router. For further information, refer to the section "Configuring SVC Traffic Parameters, on page 22" earlier in this chapter.

```
interface atm 4/0
 svc svc-1 nsap 47.0091.81.000000.0041.0B0A.1581.0040.0B0A.1585.00
 vbr-nrt 1000 500 64 800 400 64
 exit
```

Figure 7: Source and Destination Routers with Corresponding Traffic Settings



Example Creating a VC Class

The following example shows how to create a VC class named main and how to configure UBR and encapsulation parameters. For further information, refer to the sections "Creating a VC Class, on page 28" and "Configuring VC Parameters, on page 29" earlier in this chapter.

```
vc-class atm main
 ubr 10000
 encapsulation aal5mux ip
```

The following example shows how to create a VC class named sub and how to configure UBR and PVC management parameters. For further information, refer to the sections "Creating a VC Class, on page 28" and "Configuring VC Parameters, on page 29" earlier in this chapter.

```
vc-class atm sub
 ubr 15000
 oam-pvc manage 3
```

The following example shows how to create a VC class named pvc and how to configure VBR-NRT and encapsulation parameters. For further information, refer to the sections "Creating a VC Class, on page 28" and "Configuring VC Parameters, on page 29" earlier in this chapter.

```
vc-class atm pvc
 vbr-nrt 10000 5000 64
 encapsulation aal5snap
```

Examples Applying a VC Class

The following example shows how to apply the VC class named main to the ATM main interface 4/0. For further information, refer to the section "Applying a VC Class on an ATM PVC or SVC, on page 29" earlier in this chapter.

```
interface atm 4/0
 class-int main
 exit
```

The following example shows how to apply the VC class named sub to the ATM subinterface 4/0.5:

```
interface atm 4/0.5 multipoint
 class-int sub
 exit
```

The following example shows how to apply the VC class named pvc directly on the PVC 0/56:

```
interface atm 4/0.5 multipoint
 pvc 0/56
 class-vc pvc
 exit
```

Example LMI Management on an ATM PVC

The following example first shows how to configure an ILMI PVC on the main ATM interface 0/0. ILMI management is then configured on the ATM subinterface 0/0.1. For further information, refer to the section "Configuring ILMI Management, on page 32" earlier in this chapter.

```
interface atm 0/0
 pvc routerA 0/16 ilmi
 exit
!
interface atm 0/0.1 multipoint
 pvc 0/60
 ilmi manage
```

Example OAM Management on an ATM PVC

The following example shows how to enable OAM management on an ATM PVC. The PVC is assigned the name routerA and the VPI and VCI are 0 and 32, respectively. OAM management is enabled with a frequency of 3 seconds between OAM cell transmissions. For further information, refer to the section "Configuring OAM Management for PVCs, on page 34" earlier in this chapter.

```
interface atm 2/0
 pvc routerA 0/32
 oam-pvc manage 3
 oam retry 5 5 10
```

Example OAM Management on an ATM SVC

The following example shows how to enable OAM management on an ATM SVC. The SVC is assigned the name routerZ and the destination NSAP address is specified. OAM management is enabled with a frequency of 3 seconds between OAM cell transmissions. For further information, refer to the section "Configuring OAM Management for SVCs, on page 36" earlier in this chapter.

```
interface atm 1/0
 svc routerZ nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
 oam-svc manage 3
 oam retry 5 5 10
```

Examples Classical IP and ARP

This section provides three examples of classical IP and ARP configuration, one each for a client and a server in an SVC environment, and one for ATM Inverse ARP in a PVC environment.

Example Configuring ATM ARP Client in an SVC Environment

This example shows how to configure an ATM ARP client in an SVC environment. Note that the client in this example and the ATM ARP server in the next example are configured to be on the same IP network. For further information, refer to the section "Configuring the Router as an ATM ARP Client, on page 38" earlier in this chapter.

```
interface atm 2/0.5
 atm nsap-address ac.2456.78.040000.0000.0000.0000.0000.0000.0000.00
 ip address 10.0.0.2 255.0.0.0
 pvc 0/5 qsaal
 atm arp-server nsap ac.1533.66.020000.0000.0000.0000.0000.0000.0000.00
```

Example Configuring ATM ARP Server in an SVC Environment

The following example shows how to configure ATM on an interface and configures the interface to function as the ATM ARP server for the IP subnetwork. For further information, refer to the section "Configuring the Router as an ATM ARP Server, on page 39" earlier in this chapter.

```
interface atm 0/0
 ip address 10.0.0.1 255.0.0.0
 atm nsap-address ac.1533.66.020000.0000.0000.0000.0000.0000.0000.00
 atm rate-queue 1 100
 atm maxvc 1024
 pvc 0/5 qsaal
 atm arp-server self
```

Example Configuring ATM Inverse ARP in a PVC Environment

The following example shows how to configure ATM on an interface and then configures the ATM Inverse ARP mechanism on the PVCs on the interface, with Inverse ARP datagrams sent every 5 minutes on three of the PVCs. The fourth PVC will not send Inverse ATM ARP datagrams, but will receive and respond to Inverse

ATM ARP requests. For further information, refer to the section "Configuring Classical IP and ARP in an SVC Environment, on page 37" earlier in this chapter.

```
interface atm 4/0
 ip address 172.21.1.111 255.255.255.0
 pvc 0/32
 inarp 5
 exit
!
 pvc 0/33
 inarp 5
 exit
!
 pvc 0/34
 inarp 5
 exit
!
interface atm 4/0.1 point-to-point
 pvc 0/35
 exit
```

No **map-group** and **map-list** commands are needed for IP.

Examples Dynamic Rate Queue

The following examples assume that no permanent rate queues have been configured. The software dynamically creates rate queues when a **pvc** command creates a new PVC that does not match any user-configured rate queue. For further information, refer to the section "Using Dynamic Rate Queues, on page 43" earlier in this chapter.

The following example shows how to set the peak rate to the maximum that the PLIM will allow. Then it creates a rate queue for the peak rate of this VC.

```
interface 2/0
 pvc 1/41
 exit
```

The following example shows how to create a 100-Mbps rate queue with an average rate of 50 Mbps and a burst size of 64 cells:

```
interface 2/0
 pvc 2/42
 vbr-nrt 100000 50000 64
 exit
```

The following example shows how to create a 15-Mbps rate queue and set the average rate to the peak rate:

```
interface 2/0
 pvc 3/43
 ubr 15000
 exit
```

The following example shows how to configure a rate queue tolerance on the ATM interface with slot 2 and port 0. A *tolerance-value* of 20 is specified, which will apply to SVCs, discovered VCs, and PVCs.

```
interface atm 2/0
 atm rate-queue tolerance svc pvc 20
```

Example ATM Interfaces for SMDS Encapsulation

The following example shows how to create a minimal configuration of an ATM interface to support AAL3/4 and SMDS encapsulation; no protocol configuration is shown. For further information, refer to the section "Configuring ATM Subinterfaces for SMDS Networks, on page 49" earlier in this chapter.

```
interface atm 3/0
 atm aal aal3/4
 atm smds-address c140.888.9999
 atm vp-filter 0
 atm multicast e180.0999.9999
 atm pvc 30 0 30 aal34smds
```

The following example shows how IP dynamic routing might coexist with static routing of another protocol:

```
interface atm 3/0
 ip address 172.21.168.112 255.255.255.0
 atm aal aal3/4
 atm smds-address c140.888.9999
 atm multicast e180.0999.9999
 atm vp-filter 0
 atm pvc 30 0 30 aal34smds
 map-group atm
 appletalk address 10.1
 appletalk zone atm
!
 map-group atm
 atalk 10.2 smds c140.8111.1111 broadcast
```

This example shows that IP configured is dynamically routed, but that AppleTalk is statically routed. An AppleTalk remote host is configured at address 10.2 and is associated with SMDS address c140.8111.1111.

AAL3/4 associates a protocol address with an SMDS address, as shown in the last line of this example. In contrast, AAL5 static maps associate a protocol address with a PVC number.

Example Transparent Bridging on an AAL5-SNAP PVC

In the following example, three AAL5-SNAP PVCs are created on the same ATM interface. The router will broadcast all spanning tree updates to these AAL5-SNAP PVCs. No other virtual circuits will receive spanning tree updates. For further information, refer to the section "Configuring Fast-Switched Transparent Bridging, on page 51" earlier in this chapter.

```
interface atm 4/0
 ip address 10.1.1.1 255.0.0.0
 pvc 1/33
 pvc 1/34
 pvc 1/35
 bridge-group 1
!
bridge 1 protocol dec
```

Examples Inverse Multiplexing over ATM

For examples of inverse multiplexing over ATM (IMA) configuration, see the following sections:

Example E1 IMA on Multiport T1 E1 ATM Network Module

The following example shows the setup of ATM interfaces, IMA groups, PVCs, and SVCs for E1 IMA on a Multiport T1/E1 ATM Network Module:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname IMARouter
!
logging buffered 4096 debugging
!
ip subnet-zero
no ip domain-lookup
ip host 10.11.16.2
ip host 10.11.16.3
ip host 10.11.55.192
ip host 10.11.55.193
ip host 10.11.55.195
ip host 10.11.55.196
!
!
!
!
interface Ethernet0/0
 ip address 10.17.12.100 255.255.255.192
 no ip directed-broadcast
!
```

ATM interface 1/0 includes a PVC, but the specified link is not included in an IMA group. In this example, impedance and scrambling are set at their default values for E1 links and must match the far-end setting. The broadcast setting on the PVC takes precedence (addresses are fictitious).

```
interface ATM1/0
 ip address 10.1.1.26 255.255.255.1
 no ip directed-broadcast
 no atm oversubscribe
 pvc 1/40
  protocol ip 10.10.10.10 broadcast
 !
 scrambling-payload
 impedance 120-ohm
 no fair-queue
!
```

The eight-port ATM IMA E1 network module is in slot 1, and the interface commands below specify three links as members of IMA group 0.

```
interface ATM1/1
 no ip address
 no ip directed-broadcast
 no atm oversubscribe
 ima-group 0
 scrambling-payload
 impedance 120-ohm
 no fair-queue
!
interface ATM1/2
 no ip address
 no ip directed-broadcast
 no atm oversubscribe
 ima-group 0
 scrambling-payload
 impedance 120-ohm
 no fair-queue
```

```
!
interface ATM1/3
 no ip address
 no ip directed-broadcast
 no atm oversubscribe
 ima-group 0
 scrambling-payload
 impedance 120-ohm
 no fair-queue
!
```

Four links are members of IMA group 1.

```
interface ATM1/4
 no ip address
 no ip directed-broadcast
 no atm oversubscribe
 ima-group 1
 scrambling-payload
 impedance 120-ohm
 no fair-queue
!
interface ATM1/5
 no ip address
 no ip directed-broadcast
 no atm oversubscribe
 ima-group 1
 scrambling-payload
 impedance 120-ohm
 no fair-queue
!
interface ATM1/6
 no ip address
 no ip directed-broadcast
 no atm oversubscribe
 ima-group 1
 scrambling-payload
 impedance 120-ohm
 no fair-queue
!
interface ATM1/7
 no ip address
 no ip directed-broadcast
 no atm oversubscribe
 ima-group 1
 scrambling-payload
 impedance 120-ohm
 no fair-queue
!
```

The following commands specify parameters for the two IMA groups. For each group, a PVC is created and assigned an IP address.

```
interface ATM1/IMA0
 ip address 10.18.16.123 255.255.255.192
 no ip directed-broadcast
 ima clock-mode common port 2
 no atm oversubscribe
 pvc 1/42
  protocol ip 10.10.10.10 broadcast
 !
!
interface ATM1/IMA1
 ip address 10.19.16.123 255.255.255.192
 no ip directed-broadcast
 no atm oversubscribe
 ima active-links-minimum 3
 pvc 1/99
  protocol ip 10.10.10.10 broadcast
 !
!
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 10.18.16.193
ip route 10.91.0.1 255.255.255.255 10.1.0.2
no ip http server
!
!
!
line con 0
 exec-timeout 0 0
 history size 100
 transport input none
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 history size 100
```

Example T1 IMA on Multiport T1 E1 ATM Network Module

The following example shows the setup of ATM interfaces, IMA groups, PVCs, and SVCs for T1 IMA on a Multiport T1/E1 ATM Network Module:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname router
!
ip subnet-zero
!
```

There are four links in IMA group 3. The **no scrambling-payload** command is actually unnecessary, because this is the default for T1 links. The T1 automatic B8ZS line encoding is normally sufficient for proper cell delineation, so **no scrambling-payload** is the usual setting for T1 links, The scrambling setting must match the far end.

```
interface ATM0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 ima-group 3
 no scrambling-payload
 no fair-queue
!
interface ATM0/1
 ip address 10.18.16.121 255.255.255.192
 no ip directed-broadcast
 no atm ilmi-keepalive
  !
 ima-group 3
 no scrambling-payload
 no fair-queue
!
interface ATM0/2
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 ima-group 3
 no scrambling-payload
 no fair-queue
!
interface ATM0/3
 no ip address
 no ip directed-broadcast
```

```
 no atm ilmi-keepalive
 ima-group 3
 no scrambling-payload
 no fair-queue
!
```

IMA group 3 has PVCs that are set up for SVC management and signaling. Two SVCs and a communications PVC are also set up on the group interface.

```
interface ATM0/IMA3
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 pvc 0/16 ilmi
 !
 pvc 0/5 qsaal
 !
 !
 pvc first 1/43
  vbr-rt 640 320 80
  encapsulation aal5mux ip
 !
 !
 svc second nsap 47.0091810000000050E201B101.00107B09C6ED.FE
  abr 4000 3000
 !
 !
 svc nsap 47.0091810000000002F26D4901.444444444444.01
 !
```

The IMA commands below specify that three links must be active in order for the group to be operational. The common clock source is the first link, ATM 0/1, and ATM 0/2 is the test link. The differential delay maximum is set to 50 milliseconds.

```
 ima active-links-minimum 3
 ima clock-mode common 1
 ima differential-delay-maximum 50
 ima test link 2
!
interface Ethernet1/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Ethernet1/1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
no ip http server
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
!
end
```

Example T1 IMA on Multiport T1 E1 ATM Port Adapter

The following configuration example shows the setup of ATM interfaces, IMA groups, PVCs, and SVCs for T1 IMA on a Multiport T1/E1 ATM Port Adapter:

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname router
!
!
!
ip subnet-zero
!
!
```

There are four links in IMA group 3. The **no scrambling cell-payload** command is actually unnecessary, as this is the default for T1 links. Because the T1 default binary-eight zero substitution (B8ZS) line encoding is normally sufficient for proper cell delineation, this is the usual setting for T1 links, The scrambling setting must match the far-end receiver.

```
interface ATM0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 ima-group 3
 no scrambling cell-payload
 no fair-queue
!
interface ATM0/1
 ip address 10.1.1.2 255.0.0.0
 no ip directed-broadcast
 no atm ilmi-keepalive
 ima-group 3
 no scrambling-payload
 no fair-queue
!
interface ATM1/2
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 ima-group 3
 no scrambling-payload
 no fair-queue
!
interface ATM0/3
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 ima-group 3
 no scrambling-payload
 no fair-queue
!
```

IMA group 3 has PVCs that are set up for SVC management and signaling. Two SVCs and a communications PVC are also set up on the group interface.

```
interface ATM0/IMA3
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 pvc 0/16 ilmi
 !
 pvc 0/5 qsaal
```

```
 !
 !
interface ATM0/IMA3.1 point-to-point
 ip address 10.1.1.1 255.255.255.0
 pvc first 1/13
  vbr-nrt 640 320 80
  encapsulation aal5mux ip
 !
 !
svc nsap 47.0091810000000002F26D4901.444444444444.01
 !
```

The group commands below specify that three links must be active for the group to be operational. The common clock source is the first link, ATM 0/0, and ATM 0/1 is the test link. The differential delay maximum is set to 50 milliseconds (ms).

```
 ima active-links-minimum 3
 ima clock-mode common 0
 ima differential-delay-maximum 50
 ima test link 1
!
interface Ethernet1/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Ethernet1/1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
no ip http server
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
!
```

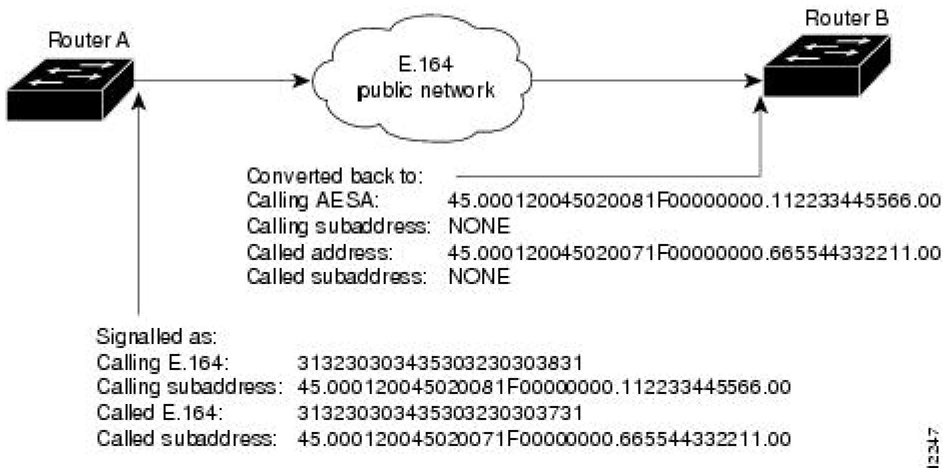
Example Configuring ATM E.164 Auto Conversion

The following example shows how to configure ATM E.164 auto conversion on an ATM interface. The figure below illustrates this example. For further information, refer to the section "Example Configuring ATM E.164 Auto Conversion, on page 119" earlier in this chapter.

```
interface atm 0 multipoint
 ip address 172.45.20.81 255.255.255.0
 pvc 0/5 qsaal
 exit
!
 atm nsap-address 45.000120045020081F00000000.112233445566.00
 atm e164 auto-conversion
 svc nsap 45.000120045020071F00000000.665544332211.00
```

```
 protocol ip 172.45.20.71
 exit
```

Figure 8: E164_AESA Address Auto Conversion Example



Upon entering an E.164 network at Router A, the destination E.164 address, extracted from the E164_AESA of the static map, is signaled in the Called Party Address. The destination E164_AESA address from the E164_AESA of the static map is signaled in the Called Party Subaddress.

The source E.164 address, extracted from the E164_AESA of the interface, is signaled in the Calling Party Address. The source E164_AESA address from the E164_AESA of the interface is signaled in the Calling Party Subaddress.

Upon leaving the E.164 network, the original Called and Calling Party addresses are extracted from the subaddresses and moved into the Called and Calling Parties. The call is then forwarded.

E164_ZDSP addresses are simply converted to E.164 addresses upon entering the E.164 network, and converted back to E164_ZDSP addresses upon leaving the network.

Examples Circuit Emulation Service

For examples of circuit emulation service (CES) configuration, see the following sections:

Example Configuring CES on a CES Network Module

In the following example, the ATM interface clock is being used. The PVC is used by AAL1 CES and is connected to a TDM group to form a CES connection. The CES connection is between ATM interface 1/0 and T1 controller 1/0 using CES PVC 1/101 and TDM group 0. TDM Group 0 has four time slots.

```
hostname vpd2005
!
logging buffered 4096 debugging
no logging console
!
!
ces 1/0
clock-select 1 em1/0
! this is the default
!
```

```
ip subnet-zero
ip host lab 172.18.207.11
ip host rtplab 172.18.207.11
ip host rtpss20 172.18.207.11
ip host dev 172.18.207.10
ip host rtpdev 172.18.207.10
!
isdn voice-call-failure 0
cns event-service server
!
controller T1 1/0
 clock source internal
 tdm-group 0 timeslots 4-8
!
controller T1 1/1
 clock source internal
 tdm-group 1 timeslots 1
!
!
interface Ethernet0/0
 ip address 172.18.193.220 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet0/1
 no ip address
 no ip directed-broadcast
!
interface Ethernet0/2
 no ip address
 no ip directed-broadcast
!
interface Ethernet0/3
 no ip address
 no ip directed-broadcast
!
interface ATM1/0
 ip address 10.7.7.7 255.255.255.0
 no ip directed-broadcast
 no atm ilmi-keepalive
 pvc 1/101 ces
 pvc 1/200
  protocol ip 10.7.7.8 broadcast
!
ip classless
ip route 10.0.0.0 0.0.0.0 Ethernet0/0
ip route 10.0.0.0 0.0.0.0 172.18.193.1
ip route 10.0.0.0 255.0.0.0 10.1.1.1
no ip http server
!
connect test ATM1/0 1/101 T1 1/0 0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password lab
 login
!
end
```

Example Configuring CES on an ATM-CES Port Adapter

The following example shows how to configure the T1 port on the ATM-CES port adapter for unstructured (clear channel) CES services. In this example, the T1 port uses adaptive clocking and the circuit name "CBR-PVC-A." For further information, refer to the section "Configuring Circuit Emulation Services, on page 79" earlier in this chapter.

```
interface cbr 6/0
```

```
 ces aal1 service unstructured
 ces aal1 clock adaptive
 atm clock internal
 ces dsx1 clock network-derived
 ces circuit 0 circuit-name CBR-PVC-A
 ces pvc 0 interface atm 6/0 vpi 0 vci 512
 no shutdown
 no ces circuit 0 shutdown
 exit
```

Example Configuring Network Clock Source Priority

The following example shows how to establish the T1 port on the ATM-CES port adapter as the first clocking priority and the ATM port as the second clocking priority. For further information, refer to the section "Configuring Network Clock Source and Priorities, on page 95" earlier in this chapter.

```
network-clock-select 1 cbr 6/0
network-clock-select 2 atm 6/0
exit
```

Example Configuring Virtual Path Shaping

The following example shows a typical configuration for the ATM-CES port adapter with VP shaping on a Cisco 7200 series router. In this example, a VP is created with the VPI value of 1 and with a peak rate of 2000 kbps. The subsequent VCs created, one data VC and one CES VC, are multiplexed onto this VP. For further information, refer to the section "Configuring Virtual Path Shaping, on page 96" earlier in this chapter.

```
interface atm 6/0
 ip address 10.2.2.2 255.255.255.0
 atm pvp 1 2000
 pvc 1/33
 no shutdown
 exit
interface cbr 6/1
 ces circuit 0
 ces pvc 0 interface atm6/0 vpi 1 vci 100
 exit
```

Example ATM Access over a Serial Interface

The following example shows how to configure a serial interface for ATM access.

In the following example, serial interface 0 is configured for ATM-DXI with MUX encapsulation. Because MUX encapsulation is used, only one protocol is carried on the PVC. This protocol is explicitly identified by a **dxi map** command, which also identifies the protocol address of the remote node. This PVC can carry IP broadcast traffic.

```
interface serial 0
 ip address 172.21.178.48
 encapsulation atm-dxi
 dxi pvc 10 10 mux
 dxi map ip 172.21.178.4 10 10 broadcast
```

Example ATM Port Adapters Connected Back-to-Back

The following example shows how to connect two ATM port adapters back to back. Two routers, each containing an ATM port adapter, are connected directly with a standard cable, which allows you to verify the operation of the ATM port or to directly link the routers to build a larger node.

By default, the ATM port adapter expects a connected ATM switch to provide transmit clocking. To specify that the ATM port adapter generates the transmit clock internally for SONET PLIM operation, add the **atm clock internal** command to your configuration.

Router A

```
interface atm 3/0
 ip address 192.168.1.10 255.0.0.0
 no keepalive
 atm clock internal
 pvc 1/35
!
 protocol ip 192.168.1.20 broadcast
```

Router B

```
interface atm 3/0
 ip address 192.168.1.20 255.0.0.0
 no keepalive
 atm clock internal
 pvc 1/35
!
 protocol ip 192.168.1.10 broadcast
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring routers that use a serial interface for ATM access through an ATM data service unit (ADSU)	"Configuring ATM Access over a Serial Interface" section in this chapter
Referencing Switched Multimegabit Data Service (SMDS) support	"SMDS Commands" chapter in the *Cisco IOS Wide-Area Networking Command Reference*
Configuring LAN emulation (LANE) for ATM	"Configuring LAN Emulation" chapter in the *Cisco IOS Switching Services Configuration Guide*
Configuring IP to ATM class of service (CoS)	"IP to ATM CoS Overview" and "Configuring IP to ATM CoS" chapters in the *Cisco IOS Quality of Service Solutions Configuration Guide*

Related Topic	Document Title
Configuring PPP over ATM	"Configuring PPP over ATM" section in the "Configuring Broadband Access: PPP and Routed Bridge Encapsulation" chapter in this book
Configuring PPP over Ethernet (PPPoE) over ATM	"Configuring PPPoE over ATM" section in the "Configuring Broadband Access: PPP and Routed Bridge Encapsulation" chapter in this book

CHAPTER 2

AAL1 CES on AIM-ATM

The AAL1 CES on AIM-ATM feature adds circuit emulation service (CES) over ATM AAL1 to Cisco 3660 and Cisco 3745 routers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for AAL1 CES on AIM-ATM

The AAL1 CES on AIM-ATM feature requires a Cisco 3660 or Cisco 3745 with an AIM-ATM or AIM-ATM-VOICE-30 installed.

Restrictions for AAL1 CES on AIM-ATM

- AIM-ATM and AIM-ATM-VOICE-30 network modules support a maximum of four T1/E1s. This can consist of two incoming and two outgoing, or three incoming and one outgoing T1/E1s. An IMA group cannot be split between multiple AIMs.
- You cannot install two AIM-ATM modules in a cellular site router. If two AIMs are needed, install one AIM-ATM and one AIM-ATM-VOICE-30.
- This feature supports only synchronous clocking. SRTS and adaptive clocking are not supported.
- This feature supports only structured CES without CAS.
- ATM subinterfaces do not support AAL1 CES.

Information About AAL1 CES on AIM-ATM

The AAL1 CES on AIM-ATM feature, along with the ATM Cell Switching and Lossless Compression R1 feature, enables wireless service providers to optimize the bandwidth used to backhaul the traffic from a cell site to the mobile central office for more efficient use of existing T1 and E1 lines.

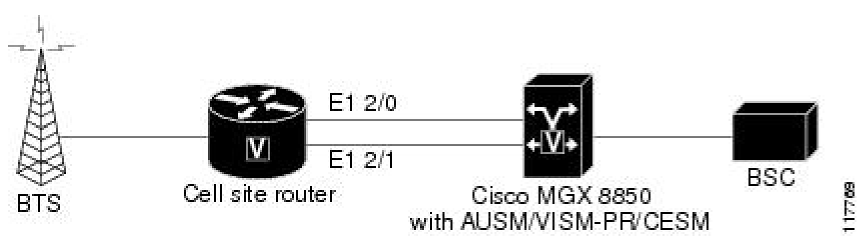
CES

CES is a technique specified by the ATM Forum for carrying constant bit-rate traffic over an ATM network. CES is a cell-based technology where voice traffic is adapted for an ATM network using AAL1, and the circuit is emulated across an ATM network.

How to Configure AAL1 CES on AIM-ATM

The sample configuration in this section is based on the figure below.

Figure 9: AAL1 CES on AIM-ATM Sample Configuration



Configuring AAL1 CES on AIM-ATM

To configure AAL1 CES on AIM-ATM, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-clock-participate slot** *number*
4. **network-clock-participate slot** *number*
5. **network-clock-participate aim** *number*
6. **controller t1** | **e1** *slot* / *port*
7. **mode atm aim** *aim-slot*
8. **controller t1** | **e1** *slot* / *port*
9. **tdm-group** *tdm-group-no* **timeslots** *timeslot-list*
10. **tdm-group** *tdm-group-no* **timeslots** *timeslot-list*
11. **interface atm** *interface-number* /*subinterface-number*
12. **pvc** *vpi* / *vci* [**ces**]
13. **ces-cdv** *time*
14. **exit**
15. **pvc** *vpi* / *vci* **ces**
16. **ces-cdv** *time*
17. **exit**
18. **exit**
19. **connect** connection-name **atm** slot/port [name of PVC/SVC | vpi/vci] **T1** slot/port TDM-group-number
20. **connect** connection-name **atm** slot/port [name of PVC/SVC | vpi/vci] **T1** slot/port TDM-group-number

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 1`	Enables the network module in the specified slot to use the network clock for its timing.

	Command or Action	Purpose
Step 4	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 2`	Enables the network module in the specified slot to use the network clock for its timing.
Step 5	**network-clock-participate aim** *number* **Example:** `Router(config)# network-clock-participate aim 0`	Specifies that the AIM in Slot 0 will derive clocking from the network source.
Step 6	**controller t1 | e1** *slot* / *port* **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode for the selected T1 or E1.
Step 7	**mode atm aim** *aim-slot* **Example:** `Router(config-controller)# mode atm aim 1`	Sets the mode of the T1 or E1 controller in AIM Slot 1.
Step 8	**controller t1 | e1** *slot* / *port* **Example:** `Router(config)# controller e1 2/0`	Enters controller configuration mode for the selected T1 or E1.
Step 9	**tdm-group** *tdm-group-no* **timeslots** *timeslot-list* **Example:** `Router(config-controller)# tdm-group 1 timeslots 1`	Configure a TDM channel group for the T1 or E1 interface. *tdm-group-no* is a value from 0 to 23 for T1 and from 0 to 30 for E1; it identifies the group. *timeslot-list* is a single number, numbers separated by commas, or a pair of numbers separated by a hyphen to indicate a range of timeslots. The valid range is from 1 to 24 for T1. For E1, the range is from 1 to 31.
Step 10	**tdm-group** *tdm-group-no* **timeslots** *timeslot-list* **Example:** `Router(config-controller)# tdm-group 2 timeslots 17-31`	Configure a TDM channel group for the T1 or E1 interface.
Step 11	**interface atm** *interface-number* /*subinterface-number* **Example:** `Router(config) # interface atm 1/0`	Enters configuration mode for the selected ATM interface.

	Command or Action	Purpose
Step 12	**pvc** *vpi* / *vci* [**ces**] **Example:** `Router(config-if)# pvc 4/44 ces`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies CES encapsulation. Enters interface-ATM-VC configuration mode.
Step 13	**ces-cdv** *time* **Example:** `Router(config-if-ces -vc)# ces-cdv 500`	Configures the cell delay variation (CDV). The configuration command has the format **ces-cdv** <time> where the time is the maximum tolerable cell arrival jitter with a range of 1 to 65535 microseconds.
Step 14	**exit** **Example:** `Router(config-if-ces-vc)# exit`	Exits back to interface configuration mode.
Step 15	**pvc** *vpi* / *vci* **ces** **Example:** `Router(config-if)# pvc 8/88 ces`	Creates a second PVC and enters interface-ATM-VC configuration mode.
Step 16	**ces-cdv** *time* **Example:** `Router(config-if-ces -vc)# ces-cdv 1000`	Configures the CDV for 1000 microseconds.
Step 17	**exit** **Example:** `Router(config-if-ces -vc)# exit`	Exits back to interface configuration mode.
Step 18	**exit** **Example:** `Router(config-if)# exit`	Exits back to configuration mode.
Step 19	**connect** connection-name **atm** slot/port [name of PVC/SVC | vpi/vci] **T1** slot/port TDM-group-number **Example:** `Router(config)# connect alpha ATM 1/0 4/44 E1 2/0 1`	Defines connections between T1 or E1 controller ports and the ATM interface.

	Command or Action	Purpose
Step 20	**connect** connection-name **atm** slot/port [name of PVC/SVC | vpi/vci] **T1** slot/port TDM-group-number **Example:** `Router(config)# connect alpha ATM 1/0 8/88 E1 2/0 2`	Defines connections between T1 or E1 controller ports and the ATM interface.

Configuring IMA Groups

To configure IMA groups, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-clock-participate** *slot number*
4. **network-clock-participate** *aim number*
5. **controller t1 | e1 slot/port**
6. **mode atm aim** *aim-slot*
7. **interface atm** *interface-number* /*subinterface-number*
8. ima-group *group-number*
9. exit
10. Repeat Step 7 through Step 9 to add ATM 2/3 to IMA group 0.
11. **interface atm** *slot* /imagroup-number
12. **pvc** *vpi* /*vci* [**ces**]
13. **partial-fill** octet
14. exit
15. **pvc** *vpi* /*vci* [**ces**]
16. **ces-cdv** *time*
17. exit
18. exit
19. **connect** connection-name **atm** slot/port [name of PVC/SVC|vpi/vci] **E1** slot/port TDM-group-number

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate** *slot number* **Example:** `Router(config)# network-clock-participate slot 2`	Enables the network module in the specified slot to use the network clock for its timing.
Step 4	**network-clock-participate** *aim number* **Example:** `Router(config)# network-clock-participate aim 0`	Specifies that the AIM in Slot 0 will derive clocking from the network source.
Step 5	**controller t1 | e1 slot/port** **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode for the selected T1 or E1.
Step 6	**mode atm aim** *aim-slot* **Example:** `Router(config-controller)#` **mode atm aim 1**	Sets the mode of the T1 or E1 controller in AIM Slot 1.
Step 7	**interface atm** *interface-number /subinterface-number* **Example:** `Router(config)#` **interface atm 2/1**	Enters configuration mode for the selected ATM interface.
Step 8	ima-group *group-number* **Example:** `Router(config-if)#` **ima-group 0**	Specifies that the link is included in an IMA group. Enter an IMA group number from 0 to 3.

	Command or Action	Purpose
Step 9	exit **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 10	Repeat Step 7 through Step 9 to add ATM 2/3 to IMA group 0.	
Step 11	**interface atm** *slot* /imagroup-number **Example:** `Router(config)#` *interface atm 0/ima0*	Enter interface configuration mode for the IMA group.
Step 12	**pvc** *vpi* /*vci* [**ces**] **Example:** `Router(config-if)# pvc 5/55 ces`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies CES encapsulation. Enters interface-ATM-VC configuration mode.
Step 13	**partial-fill** octet **Example:** `Router(config-if-ces-vc)# partial-fill 35`	Configures the number of AAL1 user octets per cell for CES. The range of values is 1-46 for T1 and 20-47 for E1. **Note** Partial fill and CDV cannot be modified under a CES PVC that is part of any connection. Do not establish the connection until after you enter the partial-fill and CDV values.
Step 14	exit **Example:** `Router(config-if-ces-vc)#` **exit**	Exits back to interface configuration mode.
Step 15	**pvc** *vpi* /*vci* [**ces**] **Example:** `Router(config-if)# pvc 6/66 ces`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies CES encapsulation. Enters interface-ATM-VC configuration mode.
Step 16	**ces-cdv** *time* **Example:** `Router(config-if-ces-vc)# ces-cdv` **1000**	Configures the CDV for 1000 microseconds.
Step 17	exit **Example:** `Router(config-if-ces-vc)#` **exit**	Exits back to interface configuration mode.

	Command or Action	Purpose
Step 18	exit **Example:** `Router(config-if)#` **exit**	Exits back to configuration mode.
Step 19	**connect** connection-name **atm** slot/port [name of PVC/SVC|vpi/vci] **E1** slot/port TDM-group-number **Example:** `Router(config)# connect alpha-IMA atm0/ima0 5/55 E1 2/0 1`	Establishes the connection between the T1 or E1 controller ports and the IMA group.

Configuration Examples for AAL1 CES on AIM-ATM

Configuring AAL1 CES on AIM-ATM Example

The following is a sample configuration for the AAL1 CES on AIM-ATM feature.

```
network-clock-participate slot 1
network-clock-participate slot 2
network-clock-participate aim 1
controller E1 2/0
 framing NO-CRC4
 clock source internal
 tdm-group 1 timeslots 1
```

Note TDM-group defined for 1 timeslot.

```
 tdm-group 2 timeslots 17-31
```

Note TDM-group defined for 15 timeslots.

```
interface ATM2/2
 scrambling-payload
 no atm ilmi-keepalive
 pvc 4/44 ces
```

Note Default CDV value set to 5 microseconds.

```
 pvc 8/88 ces
  ces-cdv 1000
```

Note Default CDV value set to 1 second.

```
connect alpha-tim ATM2/2 4/44 E1 2/0 1
connect beta-tim ATM2/2 8/88 E1 2/0 2
```

Note CES connections for TDM-AAL1 CES PVCs.

```
interface ATM2/1
 ima-group 0
 scrambling-payload
 no atm ilmi-keepalive

interface ATM2/3
 ima-group 0
 scrambling-payload
 no atm ilmi-keepalive

int atm0/ima0
pvc 5/55 ces
```

Note Default CDV value set to 5 microseconds.

```
 partial-fill 35
```

Note Range of partial-fill 1-46 for T1 or 20-47 for E1.

```
 pvc 6/66 ces
  ces-cdv 1000
connect alpha-IMA atm0/ima0 5/55 E1 2/0 1
```

Verifying the AAL1 CES on AIM-ATM Feature Example

The following shows sample output from the **show connection all** command. This command displays all ATM-TDM connections:

```
Router# show connection all
ID   Name                  Segment 1            Segment 2           State
========================================================================
.
.
2    V-220-800           E1 2/2(VOICE) 00     DSP 08/00/00        UP
4    1ds0                ATM2/2 pvc 4/44      E1 2/0 01           UP
5    V-201-801           E1 2/0(VOICE) 01     DSP 08/00/01        UP
6    seimens             ATM2/2 pvc 8/88      E1 2/0 02           UP
.
.
```

The following example shows sample output from the **show connection name** command. This command displays segments used, CDV, and partial fill values for CES connections. Default CDV is set for 5 milliseconds.

```
Router# show connection name 1ds0
Connection: 4 - 1ds0
 Current State: UP
```

```
 Segment 1:  ATM2/2 pvc 4/44
 Segment 2:  E1 2/0 01
  TDM timeslots in use: 1 (1 total)
 Internal Switching Elements: VPD
 CES-CDV: 5000 usec, Partial Fill: 0 bytes
```

The following example shows sample output from the **show atm pvc** command. This command displays all PVCs in use. It also displays the Allocated Peak Value for each connection.

```
Router# show atm pvc
           VCD /                                            Peak  Avg/Min Burst
Interface  Name         VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells Sts
2/3        TDM10         15   150  PVC    CES-AAL1 CBR     723              UP
2/3        TDM11         20   200  PVC    CES-AAL1 CBR     795              UP
```

Note Only synchronous clocking is supported.

Additional References

The following sections provide references related to the AAL1 CES on AIM-ATM feature.

Related Documents

Related Topic	Document Title
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*
Configuring voice features	*Cisco IOS Voice Configuration Library*, Release 12.4T
Configuring ATM advanced integration modules	"AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series"
Configuring high-density voice network modules	"Digital E1 Packet Voice Trunk Network Module Interfaces"

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for AAL1 CES on AIM-ATM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 4: Feature Information for AAL1 CES on AIM-ATM

Feature Name	Releases	Feature Information
AAL1 CES on AIM-ATM	12.3(8)T	The AAL1 CES on AIM-ATM feature adds circuit emulation service (CES) over ATM AAL1 to Cisco 3660 and Cisco 3745 routers. CES is a technique specified by the ATM Forum for carrying constant bit-rate traffic over an ATM network. It is a cell-based technology where voice traffic is adapted for an ATM network using AAL1, and the circuit is emulated across an ATM network. This feature, along with the ATM Cell Switching and Lossless Compression R1 feature, enables wireless service providers to optimize the bandwidth used to backhaul the traffic from a cell site to the mobile central office for more efficient use of existing T1 and E1 lines. In 12.3(8)T, this feature was introduced on the Cisco 3660 and Cisco 3745 routers. The following commands were introduced or modifief: **pvc**.

CHAPTER 3

DHCP Client on WAN Interfaces

The DHCP Client on WAN Interfaces feature extends the Dynamic Host Configuration Protocol (DHCP) to allow a DHCP client to acquire an IP address over PPP over ATM (PPPoA) and certain ATM interfaces. By using DHCP rather than the IP Control Protocol (IPCP), a DHCP client can acquire other useful information such as DNS addresses, the DNS default domain name, and the default route.

The configuration of PPPoA and Classical IP and ARP over ATM already allows for a broadcast capability over the interface (using the **broadcast** keyword on the ATM interface). Most changes in this feature are directed at removing already existing restrictions on what types of interfaces are allowed to send out DHCP packets (previously, dialer interfaces have not been allowed). This feature also ensures that DHCP RELEASE messages are sent out the interface before a connection is allowed to be broken.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for DHCP Client on WAN Interfaces

This feature works with ATM point-to-point interfaces and will accept any encapsulation type. For ATM multipoint interfaces, this feature is supported only using the aal5snap encapsulation type combined with Inverse ARP (InARP) , which builds an ATM map entry, is necessary to send unicast packets to the server (or relay agent) on the other end of the connection. InARP is supported only for the aal5snap encapsulation type.

For multipoint interfaces, an IP address can be acquired using other encapsulation types because broadcast packets are used. However, unicast packets to the other end will fail because there is no ATM map entry and thus DHCP renewals and releases also fail.

An ATM primary interface is always multipoint. An ATM subinterface can be multipoint or point-to-point.

If you are using a point-to-point interface, the routing table determines when to send a packet to the interface and ATM map entries are not needed; consequently, Inverse ARP, which builds ATM map entries, is not needed. If you are using a multipoint interface, you must use Inverse ARP to discover the IP address of the other side of the connection.

You can specify Inverse ARP through the **protocol ip inarp**interface configuration command. You must use the aal5snap encapsulation type when using Inverse ARP, because it is the only encapsulation type that supports Inverse ARP.

Information About DHCP Client on WAN Interfaces

DHCP is beneficial on WAN interfaces because it can be used to acquire information such as DNS server addresses, the DNS default domain name, and the default route.

To configure the DHCP Client on WAN Interfaces feature, you should understand the following concept:

DHCP

DHCP is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

Client computers configured to use DHCP for IP assignment do not need to have a statically assigned IP address. In addition, they generally do not need to have addresses configured for DNS servers or WINS servers, as these are also set by the DHCP server.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the need to manually assign it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

How to Configure DHCP Client on WAN Interfaces

Configuring an ATM Primary Interface Using Encapsulation and InARP

To configure an ATM primary interface (multipoint) using aal5snap encapsulation and InARP, perform the steps in this section.

```
interface atm0
  ip address dhcp
  pvc 1/100
    encapsulation aal5snap
    broadcast
    protocol ip 255.255.255.255 broadcast
     protocol ip inarp
```

Configuring an ATM Subinterface Using aa15snap Encapsulation

To configure an ATM point-to-point subinterface using aa15snap encapsulation, perform the steps in this section.

```
interface atm0.1 point-to-point
  ip address dhcp
  pvc 1/100
    encapsulation aal5snap
    broadcast
```

Configuring an ATM Subinterface Using aa15nlpid Encapsulation

To configure an ATM point-to-point subinterface using aa15nlpid encapsulation, perform the steps in this section.

```
interface atm0.1 point-to-point
  ip address dhcp
  pvc 1/100
    encapsulation aal5nlpid
    broadcast
```

Configuring an ATM Subinterface Using aa15mux PPP Encapsulation

To configure an ATM point-to-point subinterface using aa15mux PPP encapsulation, perform the steps in this section.

```
interface atm0.1 point-to-point
  pvc 1/100
  encapsulation aal5mux ppp virtual-template1
  broadcast
!
interface virtual-template1
  ip address dhcp
```

Configuration Examples for DHCP Client on WAN Interfaces

This feature has no new configuration commands; however, the **ip address dhcp**interface configuration command can now be configured on PPPoA and certain ATM interfaces.

ATM Primary Interface Using Encapsulation and InARP Example

The following example shows how to configure an ATM primary interface (multipoint) using aal5snap encapsulation and InARP.

In the following example, the **protocol ip 255.255.255.255 broadcast** configuration is needed because there must be an ATM map entry to recognize the broadcast flag on the permanent virtual circuit (PVC). You can use any ATM map entry. The **protocol ip inarp** configuration is needed so the ATM InARP can operate on the interface such that the system on the other side can be pinged once an address is assigned by DHCP.

```
interface atm0
  ip address dhcp
  pvc 1/100
    encapsulation aal5snap
    broadcast
    protocol ip 255.255.255.255 broadcast
     protocol ip inarp
```

ATM Subinterface Using aa15snap Encapsulation Example

The following example shows how to configure an ATM point-to-point subinterface using aa15snap encapsulation:

```
interface atm0.1 point-to-point
  ip address dhcp
  pvc 1/100
    encapsulation aal5snap
    broadcast
```

ATM Subinterface Using aa15nlpid Encapsulation Example

The following example shows how to configure an ATM point-to-point subinterface using aa15nlpid encapsulation:

```
interface atm0.1 point-to-point
  ip address dhcp
  pvc 1/100
    encapsulation aal5nlpid
    broadcast
```

ATM Subinterface Using aa15mux PPP Encapsulation Example

The following example shows how to configure an ATM point-to-point subinterface using aa15mux PPP encapsulation:

```
interface atm0.1 point-to-point
```

```
  pvc 1/100
  encapsulation aal5mux ppp virtual-template1
  broadcast
!
interface virtual-template1
  ip address dhcp
```

Additional References

The following sections provide references related to the feature Define Interface Policy-Map AV Pairs AAA.

Related Documents

Related Topic	Document Title
Information on Change of Authorization (CoA).	http://www.faqs.org/rfcs/rfc3576.html RFC 3576
WAN commands: complete command syntax, command mode, defaults, usage guidelines, and examples.	Cisco IOS Wide-Area Networking Command Reference
Quality of Service commands, such as show policy-map.	Cisco IOS Quality of Service Solutions Command Reference

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
http://www.faqs.org/rfcs/rfc3576.html RFC 3576	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for DHCP Client on WAN Interfaces

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 5: Feature Information for DHCP Client on WAN Interfaces

Feature Name	Releases	Feature Information
DHCP Client on WAN Interfaces	12.2(8)T	The DHCP Client on WAN Interfaces feature extends the Dynamic Host Configuration Protocol (DHCP) to allow a DHCP client to acquire an IP address over PPP over ATM (PPPoA) and certain ATM interfaces. By using DHCP rather than the IP Control Protocol (IPCP), a DHCP client can acquire other useful information such as DNS addresses, the DNS default domain name, and the default route. The following commands were introduced or modifief: **ip address dhcp**.

Glossary

LFI --link fragmentation and interleaving. Method of fragmenting large packets and then queueing the fragments between small packets.

MLP --multilink PPP.

QoS --quality of service.

VC --virtual circuit.

CHAPTER 4

Lossless Compression and ATM Cell Switching and BITS Clocking

The Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features introduce a new compression technique in DSP firmware and add enhancements to Cisco IOS that include cell switching on ATM segmentation and reassembly (SAR), and the use of an external BITS clocking source. These features enable Cisco multiservice routers to be used to transparently groom and compress traffic in a wireless service provider network and enable a service provider to optimize the bandwidth used to backhaul the traffic from a cell site to the mobile central office for more efficient use of existing T1 and E1 lines.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Lossless Compression and ATM Cell Switching and BITS Clocking

You must use a Cisco 3660 or Cisco 3745 with the following components installef:

Table 6: Supported Network Modules

Feature	Cisco 3660	Cisco 3745
Lossless compression R1	NM-HDV	NM-HDV
ATM cell switching	AIM-ATM or AIM-ATM-VOICE-30 NM-*x* FE2W with VWIC-*x* MFT-T1/E1	AIM-ATM or AIM-ATM-VOICE-30 NM-*x* FE2W with VWIC-*x* MFT-T1/E1 VWIC-*x* MFT-T1/E1 (on-board WIC slot)
BITS clocking	NM-HDV NM-*x* FE2W with VWIC-*x* MFT-T1/E1	NM-HDV NM-*x* FE2W with VWIC-*x* MFT-T1/E1 VWIC-*x* MFT-T1/E1 (on-board WIC slot)

Restrictions for Lossless Compression and ATM Cell Switching and BITS Clocking

- Operations, administration, and maintenance (OAM) cell insertion is not supported on cell-switched PVCs.
- AIM-ATM and AIM-ATM-VOICE-30 modules support a maximum of four T1/E1s. This can consist of two incoming and two outgoing, or three incoming and one outgoing T1/E1s. An IMA group cannot be split between multiple AIMs.
- Certain combinations of AIM modules can become inoperable when installed in a Cisco 3745. This problem only affects Cisco 3745 routers manufactured before June 11, 2003. See the following link for detailed information about this problem:

http://www.cisco.com/en/US/ts/fn/200/fn25194.html

- Voice activity detection (VAD) and echo cancellation are disabled when lossless compression is enabled.
- Lossless compression R1 is supported for VoATM calls with AAL2 and subcell multiplexing. VoIP calls are not supported at this time.

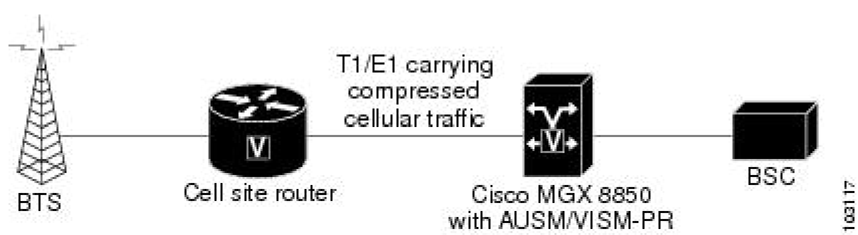
- ATM cell switching is limited to a maximum of 25 connections per AIM-ATM.
- Do not configure more than 29 LLCC channels per NM-HDV module. Configuring more than 29 LLCC channels can cause unreliable operation.
- J1 controller is not supported.
- Traffic policing is not supported.
- For Cisco 3660 routers with two NM-HDV modules installed, do not install the modules in the following slot combinations:
    - Slot 1 and Slot 3
    - Slot 2 and Slot 4
    - Slot 5 and Slot 6

Using these slot combinations can result in packet loss.

Information About Lossless Compression and ATM Cell Switching and BITS Clocking

The Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features work together to groom and compress T1 and E1 traffic between cell sites and a mobile central office. These features require a Cisco 3660 or Cisco 3745 router to be installed at the base transceiver station (BTS). This cell site router performs ATM switching and compression of cell site traffic for transport to the base station controller (BSC). A Cisco MGX 8850 with AUSM and VISM-PR terminates the T1/E1 lines that carry lossless compression codec (LLCC) traffic, converting the traffic back to PCM before passing it to the BSC. The figure below shows a sample topology that makes use of the Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features.

Figure 10: Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source Features



To configure the Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source feature, you should understand the following concepts:

Lossless Compression Codec on NM-HDV

The Lossless Compression R1 feature introduces a new compression technique in DSP firmware and the VISM card-- the lossless compression codec (LLCC). LLCC operates in a similar fashion to the existing clear channel codec: the decoded 64kbps PCM stream is a bit-exact replica of the PCM stream provided on the

TDM side of the encoding DSP. However, rather than simply packetizing the PCM stream, the LLCC encoder applies a lossless data compression scheme. This results in a net reduction in the data transmission rate, yielding a reduction in the packet transmission rate.

ATM Cell Switching on AIM-ATM and AIM-ATM-VOICE-30

The Cisco ATM Cell Switching feature enables the router to perform cell switching between two ATM connections on AIM-ATM and AIM-ATM-VOICE-30 cards, giving the router the ability to receive ATM traffic from the BTS and backhaul it to the mobile central office.

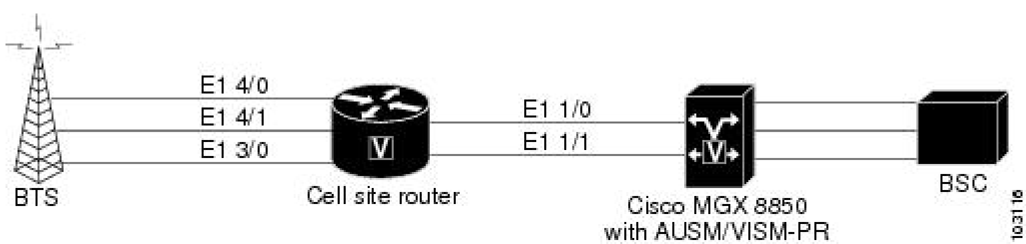
BITS Clocking on the Cisco 3660 and Cisco 3745

BITS (Building Integrated Timing Supply) network clocking enables a Cisco 3660 or Cisco 3745 router to derive network timing from the central office. BITS must be configured on the cell site router to support this feature.

How to Configure Lossless Compression and ATM Cell Switching and BITS Clocking

The instructions that follow refer to the sample configuration shown in the figure below. With this configuration, the cell site router supports three E1 connections to the BTS. Compressed cellular traffic is transported to the BSC (by way of the Cisco MGX 8850) over the E1 1/0 and E1 1/1 interfaces. Additionally, BITS clocking is derived from E1 1/1.

Figure 11: Sample Configuration



Configuring the Cell Site Router for BITS Clocking

BITS clocking enables the router at a cell site to derive timing from the mobile central office. BITS clocking ensures that data flows to a single network clock source, preventing mismatches and data slips in traffic between the BTS and the BSC. The procedure that follows configures the AIM to receive BITS clocking from E1 1/1 controller.

To configure the cell site router for BITS clocking, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-clock-participate** *slot number*
4. **network-clock-select priority** *slot number*
5. **controller t1 | e1 slot/port**
6. **clock source {line [primary | bits] | internal}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate** *slot number* **Example:** `Router(config)# network-clock-participate slot 1`	Allows the network module in the specified slot to use the network clock for its timing.
Step 4	**network-clock-select priority** *slot number* **Example:** `Router(config)# network-clock-select 1 E1 1/1`	Specifies a port to be used as a timing source for the network clock, and the priority level for the use of that port. The source that is given the highest priority is used first; if it becomes unavailable, the source with the second-highest priority is used, and so forth.
Step 5	**controller t1 | e1 slot/port** **Example:** `Router(config)# controller e1 1/1`	Enters controller configuration mode for the selected T1 or E1.
Step 6	**clock source {line [primary | bits] | internal}** **Example:** `Router(config-controller)# clock source line bits`	Specifies that the clock is generated from the T1 or E1 BITS source.

Configuring ATM Cell Switching

The procedure that follows configures the cell site router to switch ATM traffic with the Cisco MGX 8850 at the BSC. This procedure configures ATM switching between E1 3/0 and E1 1/0, using the AIM installed in Slot 1.

To configure ATM cell switching, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-clock-participate** *slot number*
4. **network-clock-participate** *slot number*
5. **network-clock-participate** *aim number*
6. **controller t1 | e1 slot/port**
7. **mode atm aim** *aim-slot*
8. **controller t1 | e1 slot/port**
9. **mode atm aim** *aim-slot*
10. **interface atm** *interface-number* / *subinterface-number*
11. **pvc** *vpi* / *vci* **l2transport**
12. **interface atm** *interface-number* / *subinterface-number*
13. **pvc** *vpi* / *vci* **l2transport**
14. **connect** *id* **atm** *slot* **.** *port-1* **atm** *slot* **.** *port-2*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate** *slot number* **Example:** `Router(config)# network-clock-participate slot 1`	Enables the network module in the specified slot to use the network clock for its timing.

	Command or Action	Purpose
Step 4	**network-clock-participate** *slot number* **Example:** `Router(config)# network-clock-participate slot 3`	Enables the network module in the specified slot to use the network clock for its timing.
Step 5	**network-clock-participate** *aim number* **Example:** `Router(config)# network-clock-participate aim 0`	Specifies that the AIM in Slot 0 will derive clocking from the network source.
Step 6	**controller t1 | e1 slot/port** **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode for the selected T1 or E1.
Step 7	**mode atm aim** *aim-slot* **Example:** `Router(config-controller)# mode atm aim 0`	Sets the mode of the T1 or E1 controller in AIM Slot 0.
Step 8	**controller t1 | e1 slot/port** **Example:** `Router(config)# controller e1 3/0`	Enters controller configuration mode for the selected T1 or E1.
Step 9	**mode atm aim** *aim-slot* **Example:** `Router(config-controller)# mode atm aim 0`	Sets the mode of the T1 or E1 controller in AIM Slot 0.
Step 10	**interface atm** *interface-number* / *subinterface-number* **Example:** `Router(config) # interface atm 1/0`	Enters configuration mode for the selected ATM interface.
Step 11	**pvc** *vpi* / *vci* **l2transport** **Example:** `Router(config-if)# pvc 10/110 l2transport`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies that the PVC is switched, not terminated.

	Command or Action	Purpose
Step 12	**interface atm** *interface-number* / *subinterface-number* **Example:** `Router (config) # interface atm 3/0`	Enters configuration mode for the selected ATM interface.
Step 13	**pvc** *vpi* / *vci* **l2transport** **Example:** `Router(config-if)# pvc 30/130 l2transport`	Creates a PVC for the VPI and VCI and specifies that the PVC is switched.
Step 14	**connect** *id* **atm** *slot* **.** *port-1* **atm** *slot* **.** *port-2* **Example:** **Example:** `Router(config)# connect Switched-Conn atm 1/0 10/110 atm 3/0 30/130`	Defines connections between T1 or E1 controller ports and the ATM interface.

Configuring the Lossless Compression Codec

The procedure that follows configures an LLCC voice channel on E1 4/0 and sends it over the ATM network using E1 1/0 and the AIM installed in Slot 1.

To configure the lossless compression codec, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-clock-participate** *slot number*
4. **network-clock-participate** *slot number*
5. **network-clock-participate** *aim number*
6. **voice service {pots | voatm | vofr | voip}**
7. **session protocol aal2**
8. **subcell-mux**
9. **codec aal2-profile custom** *profile-number* **codec**
10. **controller t1 | e1 slot/port**
11. **mode atm aim** *aim-slot*
12. **controller t1 | e1 slot/port**
13. **ds0-group** *ds0-group-number* **timeslots** *timeslot-list* **type** *signaling method*
14. **interface atm** *interface-number /subinterface-number*
15. **pvc** *vpi /vci*
16. **vbr-rt** *peak-rate average-rate burst*
17. **encapsulation aal2**
18. **dial-peer voice** *tag* **voatm**
19. **destination-pattern** *string*
20. **session protocol aal2-trunk**
21. **session target** *interface* **pvc** *vpi/vci*
22. **signal-type cas | cept | ext-signal | transparent**
23. **codec aal2-profile custom** *profile-number* **codec**
24. **voice-port** {*slot-number /subunit-number /port* | *slot /port* :*ds0-group-no* }
25. **playout-delay {fax | maximum | nominal}** *milliseconds*
26. **connection {plar | tie-line | plar-opx}** *digits* **| {trunk** *digits* **[answer-mode]}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>` **enable**	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**network-clock-participate** *slot number* **Example:** `Router(config)#` **network-clock-participate slot 1**	Enables the network module in the specified slot to use the network clock for its timing.
Step 4	**network-clock-participate** *slot number* **Example:** `Router(config)#` **network-clock-participate slot 4**	Enables the network module in the specified slot to use the network clock for its timing.
Step 5	**network-clock-participate** *aim number* **Example:** `Router(config)#` **network-clock-participate aim 0**	Specifies that the AIM in Slot 0 will derive clocking from the network source.
Step 6	**voice service {pots | voatm | vofr | voip}** **Example:** `Router(config)#` **voice service voatm**	Enters voice service configuration mode and specifies VoATM as the encapsulation type.
Step 7	**session protocol aal2** **Example:** **Router(** `config-voi-serv)#` **session protocol aal2**	Enters voice-service-session configuration mode and specifies ATM adaptation layer 2 (AAL2) trunking.
Step 8	**subcell-mux** **Example:** `Router(conf-voi-serv-sess)#` **subcell-mux**	Enables AAL2 common part sublayer (CPS) subcell multiplexing.
Step 9	**codec aal2-profile custom** *profile-number* **codec** **Example:** `Router#` **codec aal2-profile custom 51 0 0 llcc 40 0 15**	Sets the codec profile for the DSP on a per-call basis and specifies the lossless compression codec.
Step 10	**controller t1 | e1 slot/port** **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode for the selected T1 or E1.

	Command or Action	Purpose
Step 11	**mode atm aim** *aim-slot* **Example:** `Router(config-controller)# mode atm aim 0`	Sets the mode of the T1 or E1 controller in AIM Slot 0.
Step 12	**controller t1 | e1 slot/port** **Example:** `Router(config)# controller e1 4/0`	Enters controller configuration mode for the selected T1 or E1.
Step 13	**ds0-group** *ds0-group-number* **timeslots** *timeslot-list* **type** *signaling method* **Example:** `Router(config-controller)#` **ds0-group 0 timeslots 1 type ext-sig**	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type used by the router.
Step 14	**interface atm** *interface-number /subinterface-number* **Example:** `Router(config) #` **interface atm 1/0**	Enters configuration mode for the selected ATM interface.
Step 15	**pvc** *vpi /vci* **Example:** `Router(config-if-atm)#` **pvc 10/110**	Enters configuration mode for the selected PVC.
Step 16	**vbr-rt** *peak-rate average-rate burst* **Example:** `Router(config-if-atm-pvc)#` **vbr-rt 1920 1920 255**	Configures real-time variable bit rate (VBR) for VoATM voice connections.
Step 17	**encapsulation aal2** **Example:** `Router(config-if-atm-pvc)#` **encapsulation aal2**	Configures the encapsulation type for the ATM virtual circuit.
Step 18	**dial-peer voice** *tag* **voatm** **Example:** `Router(config)#` **dial-peer voice 1001 voatm**	Defines a dial-peer and specifies the method of voice encapsulation as VoATM.

	Command or Action	Purpose
Step 19	**destination-pattern** *string* **Example:** `Router(config-dial-peer)#` **destination-pattern 1001**	Specifies the prefix to be used by the dial peer.
Step 20	**session protocol aal2-trunk** **Example:** `Router(config-dial-peer)#` **session protocol aal2-trunk**	Specifies the dial peer uses AAL2 nonswitched trunk session protocol.
Step 21	**session target** *interface* **pvc** *vpi/vci* **Example:** `Router(config-dial-peer)#` **session target atm 1/0 pvc 10/100 9**	Specifies the network-specific address for the VoATM dial peer.
Step 22	**signal-type cas | cept | ext-signal | transparent** **Example:** `Router(config-dial-peer)#` **signal-type ext-signal**	Specifies that external signaling is used when connecting to the dial peer. The DSP does not generate any signaling frames.
Step 23	**codec aal2-profile custom** *profile-number* **codec** **Example:** `Router(config-dial-peer)#` **codec aal2-profile custom 51 llcc**	Sets the codec profile for the DSP on a per-call basis and specifies the lossless compression codec.
Step 24	**voice-port** {*slot-number* /*subunit-number* /*port* | *slot* /*port* :*ds0-group-no* } **Example:** `Router(config)#` **voice-port 2/0:0**	Enters voice-port configuration mode.
Step 25	**playout-delay {fax | maximum | nominal}** *milliseconds* **Example:** `Router(config-voice-port)#` **playout-delay nominal 25**	Tunes the playout buffer to accommodate packet jitter caused by switches in the WAN. The **nominal** keyword specifies the initial (and minimum allowed) delay time that the DSP inserts before playing out voice packets, in milliseconds.
Step 26	**connection {plar | tie-line | plar-opx}** *digits* **| {trunk** *digits* **[answer-mode]}**	Associates this voice-port to destination-pattern 1001.

	Command or Action	Purpose
	Example: `Router(config-voice-port)#` **connection trunk 1001**	

What to Do Next

Note To ensure that the voice-port configuration takes affect, issue the **shutdown** command, followed by **no shutdown** to enable it again.

Disabling Connection Admission Control

Connection admission control (CAC) is a set of actions taken by each ATM switch during connection setup to determine whether the requested QoS will violate the QoS guarantees for established connections. CAC reserves bandwidth for voice calls, however, the bandwidth required when LLCC is used is dynamic and usually less than what is generally reserved by CAC. Disabling CAC may help in better utilization of bandwidth when LLCC is used.

To disable CAC, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* /*subinterface-number*
4. **pvc** *vpi* /*vci*
5. **cac_off**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *interface-number /subinterface-number* **Example:** `Router(config) #` **interface atm 1/0**	Enters configuration mode for the selected ATM interface.
Step 4	**pvc** *vpi /vci* **Example:** `Router(config-if-atm)#` **pvc 10/110**	Enters configuration mode for the selected PVC.
Step 5	**cac_off** **Example:** `Router# (config-if-atm-vc)#` **cac_off**	Disables call admission control.

Verifying Lossless Compression and ATM Cell Switching and BITS Clocking

To verify the confituration use the following commands.

- **show connection all**
- **show voice dsp**
- **show voice call port-id**
- **show voice trunk supervisory summary**
- **show interfaces**

show connection all

The following example shows output from the **show connection all**command. In this example, Switched-Conn is a cell-switched connection established between PVC 10/110 and PVC 30/130, which are configured under ATM1/0 and ATM3/0 respectively.

```
Router# show connection all
ID    Name              Segment 1             Segment 2           State
========================================================================
3     V-100-700         E1 1/0(VOICE) 00      DSP 07/00/00        UP
4     V-120-700         E1 1/2(VOICE) 00      DSP 07/00/00        UP
5     Switched-Conn     ATM1/0 10/110         ATM3/0 30/130       UP
```

The **show connection all** command displays the state of Switched-Conn. If it is in the UP state, then it means the ATM cell switching connection is operational.

show voice dsp

The following example shows output from the **show voice dsp** commanf:

```
Router# show voice dsp
DSP  DSP             DSPWARE CURR  BOOT                                PAK  TX/RX
TYPE NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABORT PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ==========
C549 000 04 llcc     4.3.392 busy  idle         0 4/0:0     04     0 1752/1752
```

The **show voice dsp** command shows if the LLCC codec has been applied to the voice port. Additionally, the TX/RX COUNT indicates if packet exchange is occurring. If LLCC is operational, then TX/RX COUNT will display similar values.

show voice call *port-id*

The **show voice call**command gives detailed information about the lossless compression codec. The following example shows output from the **show voice call** commanf:

Note The **show voice call** command has a limitation that causes it to display invalid values. To ensure that accurate values are reported, invoke this command twice and look at the second output.

```
Router# show voice call 4/0:0
4/0:0 1
      vtsp level 0 state = S_CONNECTvpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
lossless compression summary:
    average compression ratio since reset       = 50
    current compression ratio                   = 50
    max buffer size (ms)                        = 41
    nominal buffer size (ms)                    = 25
    current buffer size (ms)                    = 26
    total encoder input frame count             = 5534
    total encoder output frame count            = 2767
    encoded tx front-end compressed frame count = 2767
    encoded tx back-end compressed frame count  = 0
    encoded tx frame count (no compression)     = 0
    underflow error count                       = 0
    overflow error count                        = 0
    decode error count                          = 0
    tx signalling frame count                   = 11
    rx signalling frame count                   = 10
    rx bad checksum frame count                 = 0
    rx good checksum frame count                = 2777
```

show voice trunk supervisory summary

The following example shows output from the **show voice trunk supervisory summary** commanf:

```
Router# show voice trunk supervisory summary
SLOW SCAN
4/0:0(1) : state : TRUNK_SC_CCS_CONNECT, master
```

show interfaces

The following example shows output from the **show interfaces** commanf:

```
Router# show interfaces atm1/0
ATM1/0 is up, line protocol is up
  Hardware is ATM AIM E1
  MTU 4470 bytes, sub MTU 4470, BW 1920 Kbit, DLY 20000 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Encapsulation(s): AAL5
  255 maximum active VCs, 256 VCs per VP, 0 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Per VC Queueing
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Additional References for ATM OAM Traffic Reduction

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Lossless Compression and ATM Cell Switching and BITS Clocking

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 7: Feature Information for Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

Feature Name	Releases	Feature Information
Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source	12.3(4)XD 12.3(7)T	The Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features introduce a new compression technique in DSP firmware and add enhancements to Cisco IOS that include cell switching on ATM segmentation and reassembly (SAR), and the use of an external BITS clocking source. These features enable Cisco multiservice routers to be used to transparently groom and compress traffic in a wireless service provider network and enable a service provider to optimize the bandwidth used to backhaul the traffic from a cell site to the mobile central office for more efficient use of existing T1 and E1 lines. The following commands were introduced or modifief: **cac_off**, **clock source (T1/E1 controller)**, **codec aal2-profile**, **connect (atm)**.

CHAPTER 5

ATM Multilink PPP Support on Multiple VCs

The ATM Multilink PPP Support on Multiple VCs feature facilitates traffic load balancing on high-speed virtual circuits (VCs) using multilink PPP (MLP) over Frame Relay and ATM. It also facilitates traffic load balancing by using MLP to combine packet datagrams on high-speed VCs as a means of transporting both the voice and data traffic more efficiently.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for ATM Multilink PPP Support

The ATM Multilink PPP Support on Multiple VCs feature does not support the following commands and functionality. The configuration accepts these commands, but the commands have no effect:

- **ppp interleave**

- **ppp multilink fragment-delay**

The ATM Multilink PPP Support on Multiple VCs feature does not support the link fragmentation and interleaving (LFI) functionality.

Information About ATM Multilink PPP Support

ATM Multilink PPP Support Overview

Load balancing operates at Layer 2 or Layer 3 (the network layer) of the Open System Interconnection (OSI) reference model. Layer 3 load balancing is independent of any link-layer technologies. The ATM Multilink Point-to-Point Protocol (PPP) Support on Multiple VCs feature implements load balancing at Layer 2 and depends on having MLP enabled at the link layer.

The ATM MLP functionality keeps track of packet sequencing, and this functionality buffers any packets that arrive early. With this ability, ATM MLP preserves packet order across the entire bundle.

In addition to MLP, low latency queueing (LLQ) and class-based weighted fair queueing (CBWFQ) are used to prioritize and differentiate the voice and data packets. LLQ and CBWFQ help to ensure that the voice and data traffic receive the proper quality of service (QoS) treatment (such as the correct priority queue assignment) when the voice and data traffic are transmitted.

For more information about LLQ and CBWFQ, see the *Cisco IOS Quality of Service Solutions Configuration Guide.*

Benefits of ATM Multilink PPP Support

Facilitates More Efficient Traffic Load Balancing

The ATM Multilink PPP Support on Multiple VCs feature supports the transport of real-time (voice) and other (data) traffic on Frame Relay and ATM VCs.

How to Configure ATM Multilink PPP Support

Defining the Service Policy Using the MQC

Perform this task to define the service policy using the MQC. The MQC allows you to create class maps and define service policies. Service policies are used to create classes and set match criteria for classifying traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all**| **match-any**]
4. **match ip precedence** *ip-precedence-value* [*ip-precedence-value ip-precedence-value ip-precedence-value*]
5. **exit**
6. **policy-map** *policy-name*
7. **class-map** *class-map-name* [**match-all**| **match-any**
8. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
9. **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	**class-map** *class-map-name* [**match-all**| **match-any**] **Example:** `Router(config)# class-map class1`	Specifies the name of the class map to be created and enters class-map configuration mode. If match-all or match-any value is not specified, traffic must match all the match criteria to be classified as part of the class map.
Step 4	**match ip precedence** *ip-precedence-value* [*ip-precedence-value ip-precedence-value ip-precedence-value*] **Example:** `Router(config-cmap)# match ip precedence 3 2 4`	Identifies IP precedence values as match criteria.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode.

	Command or Action	Purpose
Step 6	**policy-map** *policy-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map to be created and enters policy-map configuration mode.
Step 7	**class-map** *class-map-name* [**match-all**| **match-any** **Example:** `Router(config-pmp)# class class2`	Classifies traffic based on the class map specified and enters policy-map class configuration mode.
Step 8	**bandwidth** {*bandwidth-kbps* | **percent** *percent*} **Example:** `Router (config-pmap-c)# bandwidth 45`	Specifies a minimum bandwidth guarantee to a traffic class in periods of congestion. • A minimum bandwidth guarantee can be specified in kbps or by a percentage of the overall available bandwidth.
Step 9	**end** **Example:** `Router(config-pmp)# end`	Exits class-map configuration mode.

Defining a Multilink MLP Bundle Interface

Perform this task to define a multilink MLP bundle interface. The purpose of a multilink bundle interface is to combine more than one permanent virtual circuit (PVC). All configurations for PPP over ATM links are placed into virtual templates, and the bundle parameters are placed into the multilink bundle.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **load-interval** *seconds*
6. **no cdp enable**
7. **service-policy output** *policy-name*
8. **ppp multilink**
9. **ppp multilink fragment disable**
10. **ppp multilink group** *group-number*
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	**interface** *type* *number* **Example:** `Router(config)# interface multilink 34`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address* *mask* [**secondary**] **Example:** `Router(config-if)# ip address 209.165.201.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**load-interval** *seconds* **Example:** `Router(config-if)# load-interval 60`	Changes the length of time for which data is used to compute load statistics.
Step 6	**no cdp enable** **Example:** `Router(config-if)# no cdp enable`	Disables Cisco Discovery Protocol (CDP) on an interface.
Step 7	**service-policy output** *policy-name* **Example:** `Router(config-if)# service-policy output policy1`	Attaches the specified policy map to the output interface.
Step 8	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables MLP on an interface.

	Command or Action	Purpose
Step 9	**ppp multilink fragment disable** **Example:** `Router(config-if)# ppp multilink fragment disable`	Disables packet fragmentation.
Step 10	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink group 54`	Restricts a physical link to joining only a designated multilink-group interface.
Step 11	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Defining the Virtual Templates for Member Links

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip address**
5. **load-interval** *seconds*
6. **ppp multilink**
7. **ppp multilink group** *group-number*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface multilink 34`	Configures an interface type and enters interface configuration mode.
Step 4	**no ip address** **Example:** `Device(config-if)# no ip address`	Removes existing IP addresses or disables IP processing.
Step 5	**load-interval** *seconds* **Example:** `Device(config-if)# load-interval 30`	Changes the length of time for which data is used to compute load statistics.
Step 6	**ppp multilink** **Example:** `Device(config-if)# ppp multilink`	Enables MLP on the interface.
Step 7	**ppp multilink group** *group-number* **Example:** `Device(config-if)# ppp multilink-group 44`	Restricts a physical link to joining only a designated multilink-group interface.

Step 8	**end**
	
	Example:
	
	`Device(config-if)#`
	
	`end`
		Exits interface configuration mode.

Defining the PVCs and Bundling Member Links

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot* **/0**
   -
   -
   - **interface atm** *slot* / *port*
4. **no ip address**
5. **load interval** *seconds*
6. **atm ilmi-keepalive** [*seconds* [*retry*[*seconds*]]]
7. **pvc** [*name*] *vpi*/*vci*
8. **vbr-nrt** *output-pcr output-scr* [*output-mbs*]
9. **tx-ring-limit** *ring-limit*
10. **protocol ppp virtual-template** *number*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **interface atm** *slot* **/0** • • • **interface atm** *slot* / *port*	Specifies the ATM interface type and enters interface configuration mode.

	Command or Action	Purpose

	Example:
	`Device(config)# interface atm 2/0`
	Example:
	`or`
	Example:
	`Device(config)# interface atm 2/1`	

Step 4	**no ip address** **Example:** `Device(config-if)# no ip address`	Removes an IP address or disables IP processing.
Step 5	**load interval** *seconds* **Example:** `Device(config-if)# load interval 30`	Changes the length of time for which data is used to compute load statistics.
Step 6	**atm ilmi-keepalive** [*seconds* [*retry*[*seconds*]]] **Example:** `Device(config-if)# atm ilmi-keepalive`	Enables Interim Local Management Interface (ILMI) keepalives.
Step 7	**pvc** [*name*] *vpi*/*vci* **Example:** `Device(config-if)# pvc pvc1 0/56`	Creates an ATM PVC. Enters interface-ATM-VC configuration mode.
Step 8	**vbr-nrt** *output-pcr output-scr* [*output-mbs*] **Example:** `Device(config-if-atm-vc)# vbr-nrt 45 4 45`	Configures the variable bit rate (VBR)-non real time (NRT) QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size.
Step 9	**tx-ring-limit** *ring-limit* **Example:** `Device(config-if-atm-vc)# tx-ring-limit 3`	Limits the number of particles or packets that can be used on a transmission ring on an interface. • Use this command to tune the transmission ring to assign most of the packets to the Layer 3 queues.

	Command or Action	Purpose
Step 10	**protocol ppp virtual-template** *number* **Example:** `Device(config-if-atm-vc)# protocol ppp virtual-template 34`	Specifies that PPP is established over the ATM PVC using the configuration from the specified virtual template and enters interface configuration mode.
Step 11	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode.

Verifying ATM Multilink PPP Support

Perform this task to display information about ATM Multilink PPP Support on Multiple VCs:

SUMMARY STEPS

1. **enable**
2. **show atm pvc**
3. **show frame-relay pvc** [[**interface** *interface*] [*dlci*] [**64-bit**] | **summary** [**all**]]
4. **show interfaces**
5. **show policy-map**
6. **show ppp multilink**
7. **show queueing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm pvc** **Example:** `Device# show atm pvc`	Displays all ATM PVCs and traffic information.

	Command or Action	Purpose
Step 3	**show frame-relay pvc** [[**interface** *interface*] [*dlci*] [**64-bit**] | **summary** [**all**]] **Example:** `Device# show frame-relay pvc 16`	Displays statistics about PVCs for Frame Relay interfaces.
Step 4	**show interfaces** **Example:** `Device# show interfaces`	Displays interleaving statistics. • Interleaving data is displayed only if interleaving occurs.
Step 5	**show policy-map** **Example:** `Device# show policy-map`	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
Step 6	**show ppp multilink** **Example:** `Device# show ppp multilink`	Displays bundle information for the MLP bundles and their PPP links in the Device.
Step 7	**show queueing** **Example:** `Device# show queueing`	Lists all or selected configured queueing strategies.

Monitoring ATM Multilink PPP Support

SUMMARY STEPS

1. **enable**
2. **debug atm errors**
3. **debug atm events**
4. **debug ppp error**
5. **debug ppp multilink events**
6. **debug voice rtp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug atm errors** **Example:** `Device# debug atm errors`	Displays ATM errors.
Step 3	**debug atm events** **Example:** `Device# debug atm events`	Displays ATM events.
Step 4	**debug ppp error** **Example:** `Device# debug ppp error`	Displays information on traffic and exchanges in an internetwork implementing the PPP.
Step 5	**debug ppp multilink events** **Example:** `Device# debug ppp multilink events`	Displays information about events affecting multilink groups.
Step 6	**debug voice rtp** **Example:** `Device# debug voice RTP`	Displays information about the interleaving of voice and data packets. • The debug voice RTP command has memory overhead and should not be used when memory is scarce or when traffic is very high.

Configuration Examples for ATM Multilink PPP Support

Defining the Service Policy Using MQC Example

The following example shows how to configure a service policy using the MQC:

```
Device> enable
```

```
Device# configure terminal
Device(config)# class-map match-all DATA
Device(config-cmap)# match ip precedence 0
Device(config-cmap)# class-map match-all VOICE
Device(config-cmap)# match access-group 100
Device(config-cmap)# policy-map CISCO
Device(config-pmap)# class VOICE
Device(config-pmap-c)# priority percent 70
Device(config-pmap-c)# class DATA
Device(config-pmap-c)# bandwidth percent 5
Device(config-pmap-c)# access-list 100 permit udp any any precedence critical
```

Defining a Multilink MLP Bundle Interface Example

The following example shows how to define a multilink bundle for the mulitilink interface:

```
Device> enable
Device# configure terminal
Device(config)# interface Multilink1
Device(config-if)# ip address 10.2.1.1 255.0.0.0
Device(config-if)# load-interval 30
Device(config-if)# no cdp enable
Device(config-if)# service-policy output CISCO
Device(config-if)# ppp multilink fragment disable
Device(config-if)# ppp multilink group 1
```

Defining Virtual Templates for Member Links Example

The following example shows how to define virtual templates for member links:

```
Device> enable
Device# configure terminal
Device(config)# interface Virtual-Template1
Device(config-if)# no ip address
Device(config-if)# load-interval 30
Device(config-if)# ppp multilink
Device(config-if)# ppp multilink group 1
Device(config-if)# interface Virtual-Template2
Device(config-if)# no ip address
Device(config-if)# load-interval 30
Device(config-if)# ppp multilink
Device(config-if)# ppp multilink group 1
```

Defining PVCs and Bundling Member Links Example

The following example shows how to define and configure PVCs as bundle members:

```
Device> enable
Device# configure terminal
Device(config)# interface atm 6/0
Device(config-if)# no ip address
Device(config-if)# load-interval 30
Device(config-if)# atm ilmi-keepalive
Device(config-if)# pvc 0/34

Device(config-if-atm-vc)# vbr-nrt 1536 1536
Device(config-if-atm-vc)# tx-ring-limit 5
Device(config-if-atm-vc)# protocol ppp Virtual-Template1
Device(config-if-atm-vc)# pvc 0/35
```

```
Device(config-if-atm-vc)# vbr-nrt 800 800
Device(config-if-atm-vc)# tx-ring-limit 3
Device(config-if-atm-vc)# protocol ppp Virtual-Template2
Device(config-if-atm-vc)# pvc 0/36
Device(config-if-atm-vc)# vbr-nrt 800 400 94
Device(config-if-atm-vc)# tx-ring-limit 5
Device(config-if-atm-vc)# protocol ppp Virtual-Template1
Device(config-if-atm-vc)# pvc 0/37
Device(config-if-atm-vc)# vbr-nrt 800 800
Device(config-if-atm-vc)# tx-ring-limit 3
Device(config-if-atm-vc)# protocol ppp Virtual-Template2
Device(config-if-atm-vc)# end
```

Additional References for ATM Multilink PPP Support on Multiple VCs

The following sections provide references related to the ATM Multilink PPP Support on Multiple VCs feature.

Related Documents

Related Topic	Document Title
QoS configuration tasks	*Cisco IOS Quality of Service Solutions Configuration Guide*
QoS commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
WAN configuration tasks	*Cisco IOS Wide-Area Networking Configuration Guide*
WAN commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Wide-Area Networking Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1990	*The PPP Multilink Protocol (MP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ATM Multilink PPP Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 8: Feature Information for ATM Multilink PPP Support on Multiple VCs

Feature Name	Releases	Feature Information
ATM Multilink PPP Support on Multiple VCs	12.2(28)SB 12.2(13)T 12.2(33)SRE Cisco IOS Release XE 3.14S	The ATM Multilink PPP Support on Multiple VCs feature facilitates traffic load balancing on high-speed virtual circuits, using MLP over Frame Relay and ATM. It facilitates traffic load balancing by using MLP to combine packet datagrams on high-speed VCs, as a means for transporting both the voice and data traffic more efficiently. In Cisco IOS Release XE 3.14S, support for the ATM Multilink PPP Support on Multiple VCs feature was added on the 4451-X Integrated Services Router.

Glossary

LFI --link fragmentation and interleaving. Method of fragmenting large packets and then queueing the fragments between small packets.

MLP --multilink PPP.

QoS --quality of service.

VC --virtual circuit.

CHAPTER 6

ATM OAM Support for F5 Continuity Check

The ATM OAM Support of F5 Continuity Check feature provides the ability to detect connectivity failures at the ATM layer by introducing Operation, Administration, and Maintenance (OAM) support for F5 segment and end-to-end Continuity Check (CC) cells. This feature also enables network administrators to detect connectivity failures on each PVC. Simple Network Management Protocol (SNMP) notifications are generated when CC cells indicate virtual circuit (VC) connectivity failure and notify the administrator that continuity for a particular permanent virtual circuits (PVCs) has been lost while the PVC is still operationally up.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for ATM OAM Support for F5 Continuity Check

Extended ATM PVC and ATM OAM F5 CC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps and ATM OAM F5 CC traps can be configured. If the extended ATM PVC traps or ATM OAM F5 CC traps are enabled, you must disable them by using the **no snmp-server enable traps atm pvc extension** command before you can enable the legacy ATM PVC trap.

Restrictions for ATM OAM Support for F5 Continuity Check

Cisco digital subscriber line access multiplexers (DSLAMs) and ATM switches (such as the Cisco LS1010) do not forward F5 OAM segment CC cells.

The ATM OAM Support for F5 Continuity Check feature is supported on ATM PVCs only.

Information About ATM OAM Support for F5 Continuity Check

The ATM OAM Support for F5 Continuity Check feature introduces Operation, Administration, and Maintenance (OAM) support for the use of F5 segment and end-to-end Continuity Check (CC) cells to detect connectivity failures at the ATM layer. This feature also introduces new Simple Network Management Protocol (SNMP) notifications that are generated when CC cells indicate virtual circuit (VC) connectivity failure.

ATM OAM F5 CC cells provide an in-service tool optimized to detect connectivity problems at the VC level of the ATM layer. CC cells are sent between a router designated as the source location and a router designated as the sink location. The local router can be configured as the source, as the sink, or as both the source and the sink.

- This feature implements two types of OAM cells: CC cells for fault management and CC cells for activation and deactivation. Fault management cells detect connectivity failures. Activation and deactivation cells initiate the activation or deactivation of continuity checking.

The ATM OAM Support for F5 Continuity Check feature enables network administrators to detect connectivity failures on a per-PVC basis. The feature also provides support for SNMP notifications that notify the administrator that continuity for a particular PVC has been lost while the PVC is still operationally up.

SNMP Support for ATM OAM F5 Continuity Checking

The ATM OAM Support for F5 Continuity Check feature introduces three new SNMP notifications that indicate CC segment, CC end-to-end, and alarm indication signal/remote defect indication (AIS/RDI) failures to the Network Management System (NMS). The notifications include information such as the number of OAM failures that occurred and time stamps showing when the first and last failures occurred during the notification interval for permanent virtual circuits (PVCs). In addition to notifications, MIB tables are maintained to provide information about the failures on PVCs.

How to Configure ATM OAM Support for F5 Continuity Check

Configuring ATM OAM F5 CC Support

Perform the following steps to configure ATM OAM F5 CC support on an ATM PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*
4. **ip address** *ip-address mask*
5. **pvc** [*name*] *vpi*/*vci*
6. **oam-pvc manage cc** {**end** | **segment**} [**direction** {**both** | **sink** | **source**}] [**keep-vc-up** [**end aisrdi failure** | **seg aisrdi failure**]]
7. **oam retry cc** {**end** | **segment**} [*activation-count* [*deactivation-count* [*retry-frequency*]]]
8. **exit**

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:** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* **Example:** `Router(config)# interface atm 2/0`	Specifies an interface for configuration and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.4.9.14 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(config-if)# pvc oam 0/5`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 6	**oam-pvc manage cc** {**end** | **segment**} [**direction** {**both** | **sink** | **source**}] [**keep-vc-up** [**end aisrdi failure** | **seg aisrdi failure**]] **Example:** `Router(config-if-atm-vc)# oam pvc manage cc segment direction both`	Configures ATM OAM F5 CC management.
Step 7	**oam retry cc** {**end** | **segment**} [*activation-count* [*deactivation-count* [*retry-frequency*]]] **Example:** `Router(config-if-atm-vc)# oam retry cc end 5`	Sets the retry count and the frequency at which CC activation and deactivation requests are sent to the device at the other end of the PVC or the segment.
Step 8	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode and returns to interface configuration mode.

Configuring Denial of ATM OAM F5 CC Activation Requests

Perform the following steps to disable ATM OAM F5 CC support on an ATM PVC and to configure the PVC to deny OAM F5 CC activation requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*
4. **ip address** *ip-address mask*
5. **pvc** [*name*] *vpi*/*vci*
6. **oam-pvc manage cc** {**end** | **segment**} **deny**
7. **exit**

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	**interface atm** *number* **Example:** `Router(config)#interface atm 2/0`	Specifies an interface for configuration and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)#ip address 10.4.9.14 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(config-if)# pvc oam 0/5`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 6	**oam-pvc manage cc** {**end** | **segment**} **deny** **Example:** `Router(config-if-atm-vc)# oam-pvc manage cc end deny`	Disables ATM OAM F5 CC support by configuring the VC to deny CC activation requests.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode and returns to interface configuration mode.

Configuring ATM OAM F5 CC Deactivation Requests

Perform the following steps to configure a PVC to send ATM OAM F5 CC deactivation requests when the PVC is already down.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*
4. **ip address** *ip-address mask*
5. **pvc** [*name*] *vpi/vci*
6. **no oam-pvc manage cc** {**end** | **segment**} [**deactivate-down-vc**]
7. **exit**

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	**interface atm** *number* **Example:** `Router(config)#interface atm 2/0`	Specifies an interface for configuration and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)#ip address 10.4.9.14 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(config-if)# pvc oam 0/5`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 6	**no oam-pvc manage cc** {**end** | **segment**} [**deactivate-down-vc**] **Example:** `Router(config-if-atm-vc)# no oma-pvc manage cc end deactivate-down-vc`	Configures the PVC to send deactivation requests if the PVC is already in down state.
Step 7	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode and returns to interface configuration mode.

Configuring SNMP Notification for ATM OAM F5 CC Management

Perform the following steps to enable the MIB and send SNMP notifications that support ATM OAM F5 CC management.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps atm pvc extension mibversion 2**
4. **snmp-server enable traps atm pvc extension** {**up** | **down** | **oam failure** [**aisrdi** | **endCC** | **loopback** | **segmentCC**]}
5. **exit**

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	**snmp-server enable traps atm pvc extension mibversion 2** **Example:** `Router(config)# snmp-server enable traps atm pvc extension mibversion 2`	Specifies the MIB that supports the SNMP notifications for ATM OAM F5 CC management.
Step 4	**snmp-server enable traps atm pvc extension** {**up** | **down** | **oam failure** [**aisrdi** | **endCC** | **loopback** | **segmentCC**]} **Example:** `Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi`	Enables the sending of extended ATM PVC, ATM OAM F5 CC, ATM OAM F5 AIS/RDI, and ATM OAM F5 Loopback SNMP notifications.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits the global configuration mode and returns to privileged EXEC mode.

Verifying ATM OAM Support for F5 CC Management

To verify the configuration and operation of ATM OAM F5 CC management, perform the following steps:

SUMMARY STEPS

1. Use the **show running-config** command to verify configuration. The following is sample output for the **show running-config** command:
2. Use the **show atm pvc**command to verify that ATM OAM F5 CC management is enabled and to display the activation and deactivation retry counts and retry frequency values. This command also displays the CC state of the PVC.

DETAILED STEPS

Step 1 Use the **show running-config** command to verify configuration. The following is sample output for the **show running-config** command:

Example:

```
Router# show running-config interface atm0

Building configuration...
Current configuration :152 bytes
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 pvc 1/40
  oam-pvc manage cc segment direction both
 !
 dsl operating-mode auto
end
```

Step 2 Use the **show atm pvc**command to verify that ATM OAM F5 CC management is enabled and to display the activation and deactivation retry counts and retry frequency values. This command also displays the CC state of the PVC. The following is sample output for the **show atm pvc** command:

Example:

```
Router# show atm pvc 1/40

ATM0:VCD:1, VPI:1, VCI:40
UBR, PeakRate:0
AAL5-LLC/SNAP, etype:0x0, Flags:0xC20, VCmode:0x0
OAM frequency:0 second(s), OAM retry frequency:1 second(s)
OAM up retry count:3, OAM down retry count:5
OAM END CC Activate retry count:3, OAM END CC Deactivate retry count:3
OAM END CC retry frequency:30 second(s),
OAM SEGMENT CC Activate retry count:3, OAM SEGMENT CC Deactivate retry count:3
OAM SEGMENT CC retry frequency:30 second(s),
OAM Loopback status:OAM Disabled
OAM VC state:Not Managed
ILMI VC state:Not Managed
OAM END CC status:OAM CC Ready
OAM END CC VC state:Verified
OAM SEGMENT CC status:OAM CC Active
OAM SEGMENT CC VC state:Verified
InARP frequency:15 minutes(s)
InPkts:0, OutPkts:0, InBytes:0, OutBytes:0
InPRoc:0, OutPRoc:0, Broadcasts:0
InFast:0, OutFast:0, InAS:0, OutAS:0
Giants:0
OAM cells received:20
F5 InEndloop:0, F5 InSegloop:0,
F5 InEndcc:0, F5 InSegcc:20, F5 InAIS:0, F5 InRDI:0
F4 InEndloop:0, F4 InSegloop:0, F4 InAIS:0, F4 InRDI:0
OAM cells sent:20
F5 OutEndloop:0, F5 OutSegloop:0,
F5 OutEndcc:0, F5 OutSegcc:20, F5 OutRDI:0
F4 OutEndloop:0, F4 OutSegloop:0, F4 OutRDI:0
OAM cell drops:1
Status:UP
```

Configuration Examples for ATM OAM Support for F5 Continuity Check

ATM OAM F5 CC Support on a PVC Configuration Example

The following example shows how to configure ATM OAM CC support over the segment and configure the router to function as the source. The frequency at which CC activation and deactivation requests will be sent over the segment is also configured.

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  oam-pvc manage cc segment direction source
  oam retry cc segment 10 10 30
```

Denial of ATM OAM F5 CC Activation Requests Example

The following example shows how to disable ATM OAM F5 CC support and configure the VC to deny CC activation requests:

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  oam-pvc manage cc segment deny
```

Deactivation of ATM OAM F5 CC Deactivation Requests Example

The following example shows how to send a CC deactivation request across the segment when PVC 0/40 goes down:

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  no oam-pvc manage cc segment deactivate-down-vc
```

SNMP Notifications for ATM OAM F5 CC Configuration Example

In the following example, the ATM OAM F5 CC notifications and an extended ATM PVC notification are enabled. If CC cells detect connectivity failures on PVC 0/40, host 172.16.61.90 will receive the SNMP notifications.

```
! Configure SNMP support on your router:
snmp-server community public
snmp-server host 172.16.61.90 public
!
```

```
! Enable SNMP notifications:
snmp-server enable traps atm pvc extension mibversion 2
snmp-server enable traps atm pvc extension oam failure aisrdi
snmp-server enable traps atm pvc extension oam failure endcc
snmp-server enable traps atm pvc extension oam failure segmentcc
snmp-server enable traps atm pvc extension oam failure loopback
snmp-server enable traps atm pvc extension up
```

Additional References

The following sections provide references related to the Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature.

Related Documents

Related Topic	Document Title
Configuring PPPoA Autosense for a VC Class	Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions module
WAN commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples.	*Cisco IOS Wide-Area Networking Command Reference*
ATM commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples.	*Cisco IOS Asynchronous Transfer Mode Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Asynchronous Transfer Mode Command Reference*. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Feature Information for ATM OAM Support for F5 Continuity Check

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 9: Feature Information for ATM OAM Support for F5 Continuity Check

Feature Name	Releases	Feature Information
ATM OAM Support for F5 Continuity Check	12.2(13)T	The ATM OAM Support for F5 Continuity Check feature introduces three new SNMP notifications that indicate failures to the network management system (NMS). This feature was introduced in 12.2(13)T that supported Cisco 827 and 1700 series. The following commands were introduced or modifief: **debug atm oam cc**, **oam-pvc manage cc**, o**am-pvc manage cc deny**, **oam retry cc**, **snmp-server enable traps atm pvc extension**, **snmp-server enable traps atm pvc extension mibversion**.

Glossary

AIS --alarm indication signal. In a T1 transmission, an all-ones signal transmitted in lieu of the normal signal to maintain transmission continuity and to indicate to the receiving terminal that there is a transmission fault that is located either at or upstream from the transmitting terminal.

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system (NMS).

NMS --network management system. An application or suite of applications designed to monitor networks using SNMP.

OAM --Operation, Administration, and Maintenance. OAM cells provide a virtual-circuit-level loopback in which a router responds to the cells, demonstrating that the circuit is up and the router is operational.

PVC --permanent virtual circuit. Virtual circuit that is permanently established. In ATM terminology, PVC also stands for permanent virtual connection.

RDI --remote defect indication. In ATM, when the physical layer detects loss of signal or cell synchronization, RDI cells are used to report a virtual path connection/virtual channel connection (VPC/VCC) failure. RDI cells are sent upstream by a VPC/VCC endpoint to notify the source VPC/VCC endpoint of the downstream failure.

SNMP --Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents and is used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

SNMP trap --Message from an SNMP agent alerting the SNMP manager to a condition on the network.

CHAPTER 7

ATM OAM Ping

The ATM OAM Ping feature sends an ATM Operation, Administration, and Maintenance (OAM) packet to confirm the connectivity of a specific permanent virtual circuit (PVC). The status of the PVC is displayed when a response to the OAM packet is received. The ATM OAM Ping feature allows the network administrator to verify PVC integrity and facilitates ATM network troubleshooting.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for the ATM OAM Ping Feature

A PVC corresponding to the virtual path identifier (VPI) and virtual channel identifier (VCI) values entered with the **ping** command should already exist. (For Cisco 827 series routers, the virtual circuit need not exist.)

For information about how to configure ATM PVCs, see the section "Configuring PVCs" in the chapter "Configuring ATM" in the *Cisco IOS Asynchronous Transfer Mode Configuration Guide*.

Restrictions for the ATM OAM Ping Feature

The ATM OAM Ping feature does not support pings based on the following:

- Network service access point (NSAP) addresses
- Multiple-hop loopbacks
- Loopback location identification

Information About the ATM OAM Ping Feature

Benefits of the ATM OAM Ping Feature

The ATM OAM Ping feature modifies the **ping**command, which can be used to send an OAM packet to verify PVC connectivity. The status of the PVC is displayed when a response to the OAM packet is received. This is a common method for testing the accessibility of devices.

The **ping atm interface atm** command provides two ATM OAM ping options:

- End loopback--Verifies end-to-end PVC integrity.
- Segment loopback--Verifies PVC integrity to the immediate neighboring ATM device.

The **ping atm interface atm** command is used to determine the following:

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

The simpler **ping** command provides an interactive mode for testing ATM network connectivity. The **ping** command first sends an OAM command loopback cell to the destination and then waits for an OAM response loopback cell. The ping is successful only when the following criteria are met:

- The OAM command loopback cell reaches the destination.
- The destination is able to send an OAM loopback response cell back to the source within a predetermined time called a *timeout* . The default value of the timeout is 2 seconds on Cisco routers.

How to Use the ATM OAM Ping Feature

Testing Network Connectivity Using Ping in Normal Mode

This section describes how to test the network connectivity by using the **ping atm interface atm** command in normal mode; that is, by entering all values for the **ping** test on the command line.

SUMMARY STEPS

1. **enable**
2. **ping atm interface atm** *interface-number* *vpi-value* [*vci-value* [**end-loopback** | **seg-loopback**] [*repeat* [*timeout*]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ping atm interface atm** *interface-number* *vpi-value* [*vci-value* [**end-loopback** | **seg-loopback**] [*repeat* [*timeout*]]] **Example:** `Router# ping atm interface atm 1/1.1 0 500 end-loopback 1 2`	Displays a response to confirm the connectivity of a specific PVC.

Testing Network Connectivity Using Ping in Interactive Mode

This section describes how to test network connectivity by using the **ping** command; that is, by providing values for the **ping** test by typing the value after the prompts displayed and pressing the **Enter** key. Press the **Enter** key without supplying a value to use the default.

SUMMARY STEPS

1. **enable**
2. **ping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**ping** **Example:** `Router#` **ping**	Displays a response to confirm the connectivity of a specific PVC.

Aborting a Ping Session

To terminate a ping session, type the escape sequence **Ctrl-Shift-6**.

Configuration Examples for ATM OAM Ping

Verifying the Connectivity of a Specific PVC Example

The following example verifies the connectivity of a specific PVC by sending an ATM OAM packet and confirms the connectivity when it is successful:

```
Router# show
atm pvc 0/500
VC 0/500 doesn't exist on interface ATM1/0 - cannot display
ATM1/1.1: VCD: 2, VPI: 0, VCI: 500
UBR, PeakRate: N/A (UBR VC)
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0
OAM frequency: 10 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM END CC Activate retry count: 3, OAM END CC Deactivate retry count: 3
OAM END CC retry frequency: 30 second(s),
OAM SEGMENT CC Activate retry count: 3, OAM SEGMENT CC Deactivate retry count: 3
OAM SEGMENT CC retry frequency: 30 second(s),
OAM Loopback status: OAM Received
OAM VC state: Verified
ILMI VC state: Not Managed
OAM END CC status: OAM CC Ready
OAM END CC VC state: Verified
OAM SEGMENT CC status: OAM CC Ready
OAM SEGMENT CC VC state: Verified
VC is managed by OAM.
InARP frequency: 15 minutes(s)
InPkts: 289035, OutPkts: 217088, InBytes: 21165546, OutBytes: 17367793
InPRoc: 289039, OutPRoc: 289274
InFast: 0, OutFast: 0, InAS: 1, OutAS: 2
Out CLP=1 Pkts: 0
OAM cells received: 119900
F5 InEndloop: 119809, F5 InSegloop: 0,
F5 InEndcc: 0, F5 InSegcc: 0, F5 InAIS: 92, F5 InRDI: 0
OAM cells sent: 119902
F5 OutEndloop: 119810, F5 OutSegloop: 0,
F5 OutEndcc: 0, F5 OutSegcc: 0, F5 OutAIS: 0, F5 OutRDI: 92
OAM cell drops: 0
Status: UP
```

Testing Network Connectivity Using Ping in Normal Mode Example

The following is sample output for the **ping atm interface atm**command in normal mode:

```
Router# ping atm interface atm1/1.1 0 500
Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/16/52 ms
Router# ping atm interface atm1/1.1 0 500 seg-loopback
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router# ping atm interface atm1/1.1 0 500 end-loopback 100 25
Type escape sequence to abort.
Sending 100, 53-byte end-to-end OAM echoes, timeout is 25 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/13/180 ms
Router# ping atm interface atm1/1.1 0 500 seg-loopback 50 20
Type escape sequence to abort.
Sending 50, 53-byte segment OAM echoes, timeout is 20 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 1/1/4 ms
Router# show atm pvc 0/500
VC 0/500 doesn't exist on interface ATM1/0 - cannot display
ATM1/1.1: VCD: 2, VPI: 0, VCI: 500
UBR, PeakRate: N/A (UBR VC)
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0
OAM frequency: 10 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM END CC Activate retry count: 3, OAM END CC Deactivate retry count: 3
OAM END CC retry frequency: 30 second(s),
OAM SEGMENT CC Activate retry count: 3, OAM SEGMENT CC Deactivate retry count: 3
OAM SEGMENT CC retry frequency: 30 second(s),
OAM Loopback status: OAM Received
OAM VC state: Verified
ILMI VC state: Not Managed
OAM END CC status: OAM CC Ready
OAM END CC VC state: Verified
OAM SEGMENT CC status: OAM CC Ready
OAM SEGMENT CC VC state: Verified
VC is managed by OAM.
InARP frequency: 15 minutes(s)
InPkts: 290975, OutPkts: 219031, InBytes: 21306632, OutBytes: 17509085
InPRoc: 290979, OutPRoc: 291219
InFast: 0, OutFast: 0, InAS: 1, OutAS: 2
Out CLP=1 Pkts: 0
OAM cells received: 120881
F5 InEndloop: 120734, F5 InSegloop: 55,
F5 InEndcc: 0, F5 InSegcc: 0, F5 InAIS: 92, F5 InRDI: 0
OAM cells sent: 120882
F5 OutEndloop: 120735, F5 OutSegloop: 55,
F5 OutEndcc: 0, F5 OutSegcc: 0, F5 OutAIS: 0, F5 OutRDI: 92
OAM cell drops: 0
Status: UP
```

Testing Network Connectivity Using Ping in Interactive Mode Example

The following is sample output for the **ping**command in the interactive mode:

```
Router# ping
Protocol [ip]: atm
ATM Interface: atm1/1.1
```

```
VPI value [0]: 0
VCI value [1]: 500
Loopback - End(0), Segment(1) [0]:
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/12 ms
```

Additional References

The following sections provide references related to the ATM OAM Ping feature.

Related Documents

Related Topic	Document Title
Configuring PVCs and mapping a protocol address to a PVC while configuring ATM	Configuring PVCs section of *Cisco IOS Configuring ATM Feature Guide*
Configuring ATM	*Cisco IOS Configuring ATM Feature Guide*
ATM commands, complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Asynchronous Transfer Mode Command Reference*
Configuring ATM OAM traffic reduction	"ATM OAM Traffic Reduction" feature module
Configuring PVCs with or without OAM	"Using OAM for PVC Management" sample configuration
Detecting failures when using OAM cells and PVC management	Troubleshooting PVC Failures When Using OAM Cells and PVC Management technical note
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
ITU-T Specification I.610 (ITU-T specification for B-ISDN operation and maintenance principles and functions).	I.610 Series I: Integrated Services Digital Network Maintenance principles

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the ATM OAM Ping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 10: Feature Information for ATM OAM Ping

Feature Name	Releases	Feature Information
ATM OAM Ping	12.0(21)S 12.2(28)SB 12.2(18)SXE 12.2(33)SRE 12.2(13)T	The ATM OAM Ping feature lets the router automatically detect when a peer ATM interface is in loopback mode. When loopback is detected on an interface where end-to-end F5 OAM is enabled, the impacted PVC is moved to a DOWN state, and traffic is suspended. When the loopback condition in the peer ATM interface is removed, the PVC is moved back to an UP state. The following command was introduced: **ping atm interface atm**

CHAPTER 8

ATM Policing by Service Category for SVC SoftPVC

The ATM Policing by Service Category for SVC/SoftPVC feature enables you to specify which traffic to police, based on service category, on switched virtual circuits (SVCs) or terminating virtual circuits (VCs) on the destination end of a soft VC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About ATM Policing by Service Category

When configured, an ATM switch at the network side of a user-to-network (UNI) interface polices the flow of cells in the forward (into the network) direction of a virtual connection. These traffic policing mechanisms are known as usage parameter control (UPC). With UPC, the switch determines whether received cells comply with the negotiated traffic management values and takes one of the following actions on violating cells:

- Pass the cell without changing the cell loss priority (CLP) bit in the cell header.
- Tag the cell with a CLP bit value of 1.
- Drop (discard) the cell.

This feature enables you to select which traffic is affected by UPC and how it is affected. For example, you can configure your switch to pass all UBR traffic, but tag all other traffic types.

For more information about UPC, see the "Traffic and Resource Management" chapter in the *Guide to ATM Technology* .

How to Configure ATM Policing by Service Category

Configuring ATM Policing by Service Category

The task in this section configures the ATM Policing by Service Category for SVC/SoftPVC feature, using the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port*
4. **atm svc-upc-intent [{abr | cbr | vbr-rt | vbr-nrt | ubr}] {tag | pass | drop}**

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.

	Command or Action	Purpose
Step 3	**interface atm** *slot* / *subslot* / *port* **Example:** `Router(config)#` **interface atm** *slot*/*subslot*/*port*	Selects the ATM interface.
Step 4	**atm svc-upc-intent [{abr | cbr | vbr-rt | vbr-nrt | ubr}] {tag | pass | drop}** **Example:** `Router(config-if)#` **atm svc-upc-intent** [{**abr** | **cbr** | **vbr-rt** | **vbr-nrt** | **ubr**}] {**tag** | **pass** | **drop**} **Example:** **Example:** `(Repeat this step for each service category and UPC mode combination.)`	Specifies the UPC mode. If no service category is specified, then the UPC mode configuration is applied to all traffic types.

Verifying ATM Policing by Service Category

SUMMARY STEPS

1. Enter the **show atm vc** or **show atm vp** EXEC command to display the UPC mode for a particular virtual circuit or VP.
2. Enter the **show atm interface** EXEC command. If the UPC mode is not the same for all service categories, the "Svc Upc Intent" field displays "by sc."

DETAILED STEPS

Step 1 Enter the **show atm vc** or **show atm vp** EXEC command to display the UPC mode for a particular virtual circuit or VP.

Example:

```
Switch# show atm vc int atm 0/0/1 2 120
Interface:ATM0/0/1, Type:oc3suni
VPI = 2  VCI = 120
Status:DOWN
Time-since-last-status-change:1w1d
Connection-type:PVC
Cast-type:point-to-multipoint-leaf
```

```
Packet-discard-option:disabled
Usage-Parameter-Control (UPC):pass

Wrr weight:2
Number of OAM-configured connections:0
OAM-configuration:disabled
OAM-states: Not-applicable
Cross-connect-interface:ATM0/0/1, Type:oc3suni
...
```

Step 2 Enter the **show atm interface** EXEC command. If the UPC mode is not the same for all service categories, the "Svc Upc Intent" field displays "by sc."

Example:

```
Switch# show atm interface atm 8/0/1
Interface:     ATM8/0/1        Port-type:     oc3suni
IF Status:     UP              Admin Status:  up
Auto-config:   enabled         AutoCfgState:  completed
IF-Side:       Network         IF-type:       NNI
Uni-type:      not applicable  Uni-version:   not applicable
Max-VPI-bits:  8               Max-VCI-bits:  14
Max-VP:        255             Max-VC:        16383
ConfMaxSvpcVpi:255             CurrMaxSvpcVpi:255
ConfMaxSvccVpi:255             CurrMaxSvccVpi:255
ConfMinSvccVci:35              CurrMinSvccVci:35
Svc Upc Intent:by sc
           Signalling:    Enabled
ATM Address for Soft VC:47.0091.8100.0000.0002.b9ae.9301.4000.0c84.0010.00
Configured virtual links:
  PVCLs SoftVCLs   SVCLs   TVCLs   PVPLs SoftVPLs   SVPLs Total-Cfgd Inst-Conns
      3        4       0       0       1        0       0          8          7
Logical ports(VP-tunnels):    0
Input cells:   3036674         Output cells:  3036816
5 minute input rate:            0 bits/sec,       0 cells/sec
5 minute output rate:           0 bits/sec,       0 cells/sec
Input AAL5 pkts:1982638, Output AAL5 pkts:1982687, AAL5 crc errors:0
```

Troubleshooting Tips

If a VC is not configured with the appropriate UPC mode, make sure that the VC was set up after the **atm svc-upc-intent** command was configured. Changes to the UPC mode take effect after the VC is torn down and set up again.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router(config)# **interface atm***slot*/*subslot*/*port*
4. Router(config-if)# **atm svc-upc-intent** [{**abr** | **cbr** | **vbr-rt** | **vbr-nrt** | **ubr**}] {**tag** | **pass** | **drop**}
5. Repeat step 4 for each service category and UPC mode combination.

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	Router(config)# **interface atm***slot*/*subslot*/*port*	Selects the ATM interface.
Step 4	Router(config-if)# **atm svc-upc-intent** [{**abr** | **cbr** | **vbr-rt** | **vbr-nrt** | **ubr**}] {**tag** | **pass** | **drop**}	Specifies the UPC mode. • If no service category is specified, then the UPC mode configuration is applied to all traffic types.
Step 5	Repeat step 4 for each service category and UPC mode combination.	--

Monitoring and Maintaining ATM Policing by Service Category

The task in this section enable you to monitor and maintain the ATM Policing by Service Category for SVC/SoftPVC feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router# **show atm interface**
4. Router# **show controllers atm***slot*/*subslot*/*port*
5. Router# **show atm vc** [**interface atm***slot*/*subslot*/*port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router# **show atm interface**	Displays ATM-specific information about an ATM interface.
Step 4	Router# **show controllers atm***slot***/***subslot***/***port*	Displays information about a physical port device. Includes dropped (or discarded) cells.
Step 5	Router# **show atm vc** [**interface atm***slot***/***subslot***/***port*]	Displays the configured UPC action and intelligent packet discard mechanisms, as well as the number of cells discarded because of UPC violations.

Configuration Examples for ATM Policing by Service Category

Non-UBR Traffic Policing Example

In the following example, the UBR traffic on ATM 3/0/0 is passed while all other traffic is policef:

```
Router(config)# interface atm 3/0/0
Router(config-if)# atm svc-upc-intent ubr pass
Router(config-if)# atm svc-upc-intent cbr tag
Router(config-if)# atm svc-upc-intent vbr-rt tag
Router(config-if)# atm svc-upc-intent vbr-nrt tag
Router(config-if)# atm svc-upc-intent abr drop
```

Monitoring and Maintaining ATM Policing by Service Category Example

```
Switch# show atm vc interface atm 3/0/1.51 51 16

     Interface: ATM3/0/1.51, Type: oc3suni
     VPI = 51  VCI = 16
     Status: DOWN
     Time-since-last-status-change: 2w0d
     Connection-type: PVC
     Cast-type: point-to-point
     Packet-discard-option: enabled

     Usage-Parameter-Control (UPC): pass

     Wrr weight: 32
```

```
Number of OAM-configured connections: 0
OAM-configuration: disabled
OAM-states:  Not-applicable
Cross-connect-interface: ATM2/0/0, Type: ATM Swi/Proc
Cross-connect-VPI = 0
Cross-connect-VCI = 73
Cross-connect-UPC: pass
Cross-connect OAM-configuration: disabled
Cross-connect OAM-state:  Not-applicable
Encapsulation: AAL5ILMI
Threshold Group: 6, Cells queuef: 0
Rx cells: 0, Tx cells: 0
Tx Clp0:0,  Tx Clp1: 0
Rx Clp0:0,  Rx Clp1: 0
Rx Upc Violations:0, Rx cell drops:0

Rx pkts:0, Rx pkt drops:0
Rx connection-traffic-table-index: 6
Rx service-category: UBR (Unspecified Bit Rate)
Rx pcr-clp01: 424
Rx scr-clp01: none
Rx mcr-clp01: none
Rx      cdvt: 1024 (from default for interface)
Rx       mbs: none
Tx connection-traffic-table-index: 6
Tx service-category: UBR (Unspecified Bit Rate)
Tx pcr-clp01: 424
Tx scr-clp01: none
Tx mcr-clp01: none
Tx      cdvt: none
Tx       mbs: none
No AAL5 connection registered
```

Additional References

The following sections provide references related to the OAM Segment Endpoint feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ATM Commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*
Any Transport over MPLS	Any Transport over MPLS
Detecting failures when using OAM cells and PVC management	http://www.cisco.com/en/US/tech/tk39/tk48/technologies_tech_note09186a008009461c.shtml Troubleshooting PVC Failures When Using OAM Cells and PVC Management
Layer 2 Tunnel Protocol Version 3	Layer 2 Tunnel Protocol Version 3
WAN configuration	*Cisco IOS Wide-Area Networking Configuration Guide*

Standards

Standards[21]	Title
IETF Specification	*Encapsulation Methods for Transport of Layer 2 Frames over MPLS*
IETF Specification	*Layer Two Tunneling Protocol (Version 3)*
IETF Specification	*Transport of Layer 2 Frames over MPLS*
ITU-T Specification I.610 (ITU-T specification for B-ISDN operation and maintenance principles and functions)	*I.610 Series I:* B-ISDN Operation and Maintenance Principles and Functions

21 Not all supported standards are listed.

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2661	*Layer Two Tunneling Protocol* "L2TP"
RFC 3032	*MPLS Label Stack Encoding*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Asynchronous Transfer Mode Command Reference*. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List*.

- **atm svc-upc-intent**

Feature Information for ATM Policing by Service Category

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 11: Feature Information for ATM Policing by Service Category for SVC/SoftPVC

Feature Name	Releases	Feature Information
ATM Policing by Service Category for SVC/SoftPVC	12.2(4)B 12.2(13)T	The ATM Policing by Service Category for SVC/SoftPVC feature enables you to specify which traffic to police, based on service category, on switched virtual circuits (SVCs) or terminating VCs on the destination end of a soft VC. In 12.2(4)B, this feature was introduced on the Cisco 6400 NSP. This feature was integrated into Cisco IOS release 12.2 (13) T.

Glossary

ABR --available bit rate. QoS class defined by the ATM Forum for ATM networks. ABR is used for connections that do not require timing relationships between source and destination. ABR provides no guarantees in terms of cell loss or delay, providing only best-effort service. Traffic sources adjust their transmission rate in response to information they receive describing the status of the network and its capability to successfully deliver data. Compare with CBR, UBR, and VBR.

CBR --constant bit rate. QoS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery. Compare with ABR, UBR, and VBR.

CLP --cell loss priority. Field in the ATM cell header that determines the probability of a cell being dropped if the network becomes congested. Cells with CLP = 0 are insured traffic, which is unlikely to be dropped. Cells with CLP = 1 are best-effort traffic, which might be dropped in congested conditions to free up resources to handle insured traffic.

PVC --permanent virtual circuit (or connection). Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection. Compare with SVC. See also virtual circuit.

soft PVC --A PVC-SVC hybrid in which only the two terminating virtual connection links (VCLs) at either end are permanent and the rest of the VCLs are switched (SVC). Like the PVC, a soft PVC is permanent and the called party cannot drop the connection. Like the SVC, a soft PVC is automatically rerouted if a switch or link in the path fails.

SVC --switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. See also virtual circuit. Called a switched virtual connection in ATM terminology. Compare with PVC.

tagged traffic --ATM cells that have their CLP bit set to 1. If the network is congested, tagged traffic can be dropped to ensure the delivery of higher-priority traffic. Sometimes called DE traffic. See also CLP.

traffic policing --Process used to measure the actual traffic flow across a given connection and compare it to the total admissible traffic flow for that connection. Traffic outside of the agreed upon flow can be tagged (where the CLP bit is set to 1) and can be discarded en route if congestion develops. Traffic policing is used in ATM, Frame Relay, and other types of networks. Also known as admission control, permit processing, rate enforcement, and UPC. See also tagged traffic.

UBR --unspecified bit rate. QoS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network but there are no guarantees in terms of cell loss rate and delay. Compare with ABR, CBR, and VBR.

UPC --usage parameter control. See traffic policing.

VBR --variable bit rate. QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

virtual circuit --Logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC). Virtual circuits are used in Frame Relay and X.25. In ATM, a virtual circuit is called a virtual channel. Sometimes abbreviated VC.

CHAPTER 9

Configuring ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements feature provides the ability to send Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) when the PVC state changes and when Operations, Administration and Maintenance (OAM) loopback fails for a PVC. This feature also provides information about the virtual path identifier/virtual channel identifier (VPI/VCI) in the ATM PVC traps.

The ATM OAM AIS-RDI Monitoring feature extends the existing ATM virtual circuit OAM functionality to include monitoring of the Alarm Indication Signal-Remote Defect Indication (AIS-RDI).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for ATM SNMP Trap and OAM Enhancements

Before you enable ATM PVC trap support, you must configure SNMP support and an IP routing protocol on your router. For more information about configuring SNMP support, refer to the chapter "Configuring SNMP Support" in the *Cisco IOS Network Management Configuration Guide* .

To receive PVC failure notification and to allow access to PVC status tables on your router, you must have the Cisco extended ATM PVC trap MIB called CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my compiled in your Network Management System (NMS) application. You can find this MIB on the Web at Cisco's MIB website that has the URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before configuring extended ATM PVC traps.

Restrictions for ATM SNMP Trap and OAM Enhancements

- Extended ATM PVC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before configuring extended ATM PVC traps.
- ATM PVC UP traps are not generated for newly created PVCs. They are only generated for PVCs that go from the DOWN state to the UP state.

Information About ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements feature introduces the following enhancements to the SNMP notifications for ATM permanent virtual circuits (PVCs) and to OAM functionality:

- ATM PVC traps will be generated when the operational state of a PVC changes from the DOWN to UP state.
- ATM PVC traps will be generated when OAM loopback fails and the PVC will remain in the UP state, rather than going down.
- The ATM PVC traps are now extended to include virtual path identifier/virtual channel identifier (VPI/VCI) information, the number of state transitions a PVC goes through in an interval, and the time stamp of the first and the last PVC state transition.

Before configuring ATM SNMP traps and OAM VC enhancements, you should understand the following concepts:

Benefits of Configuring ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements and the ATM OAM AIS-RDI Monitoring features have the following benefits:

- Enables you to use SNMP to detect the recovery of PVCs that are down.
- Enables you to use SNMP to detect when OAM loopback fails for a PVC.

- Keeps the PVC in the UP state when OAM loopback fails, to allow continuous flow of data.
- Provides VPI/VCI information in the ATM PVC traps, to let you know the PVC that changed operational state or encountered an OAM loopback failure.
- Provides statistics on the number of state transitions a PVC goes through.
- Provides flexibility to control the status change of PVC when a faulty condition is detected on VC and OAM VC-AIS cells are generated.

ATM OAM AIS-RDI Monitoring

The ATM OAM AIS-RDI Monitoring feature extends the existing ATM VC OAM functionality to include monitoring of the AIS-RDI. Once the feature is enabled, OAM AIS-RDI is monitored on the VCs. If the number of consecutive OAM AIS-RDI cells received is greater than a configurable number, the VC is brought down. The VC is brought up when there are no OAM AIS-RDI cells received within a configurable interval.

ATM PVC Up Trap

Before the introduction of the ATM SNMP trap and OAM enhancements, the only SNMP notifications for ATM PVCs were the ATM PVC failure traps that were generated when a PVC failed or left the UP operational state. The ATM SNMP trap and OAM enhancements introduce ATM PVC up traps, which are generated when a PVC changes from the DOWN to the UP state.

ATM PVC OAM Failure Trap

The ATM SNMP trap and OAM enhancements feature introduces the ATM PVC OAM failure trap. OAM loopback is a mechanism that detects whether a connection is up or down by sending OAM end-to-end loopback command/response cells. An OAM loopback failure indicates that the PVC has lost connectivity. The ATM PVC OAM failure trap is generated when OAM loopback for a PVC fails and is sent at the end of the notification interval.

When OAM loopback for a PVC fails, the PVC is included in the atmStatusChangePVclRangeTable or atmCurrentStatusChangePVclTable and in the ATM PVC OAM failure trap.

Before this feature was introduced, if OAM loopback failed, the PVC was being placed in the DOWN state. When the ATM PVC OAM failure trap is enabled, the PVC remains up even if OAM loopback fails, and thus it ensures continuous flow of data.

Note ATM PVC traps are generated at the end of the notification interval. It is possible to generate three types of ATM PVC traps (the ATM PVC failure trap, ATM PVC up trap, and ATM PVC OAM failure trap) at the end of the same notification interval. However, only one type of trap is generated for each PVC.

Extended ATM PVC Traps

The ATM SNMP Trap and OAM Enhancements feature introduces extended ATM PVC traps. The extended traps include VPI/VCI information for affected PVCs, the number of up-to-down and down-to-up state transitions a PVC goes through in an interval, and the time stamp of the first and the last PVC state transition.

Note Extended ATM PVC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before configuring extended ATM PVC traps.

Supported MIB Objects and Tables

The ATM PVC trap is defined in the ATM PVC trap MIB. The ATM SNMP trap and OAM enhancements introduce the following MIB objects and tables:

- The table atmInterfaceExt2Table displays the status of ATM PVCs and is indexed by ifIndex. This table contains the following objects:
  - atmIntfCurrentlyDownToUpPVcls
  - atmIntfOAMFailedPVcls
  - atmIntfCurrentlyOAMFailingPVcls
- The table atmCurrentStatusChangePVclTable displays information about ATM PVCs that undergo through an operational state change and is indexed by ifIndex, atmVclVpi, and atmVclVci. This table contains the following objects:
  - atmPVclStatusTransition
  - atmPVclStatusChangeStart
  - atmPVclStatusChangeEnd
- The table atmStatusChangePVclRangeTable displays information about ATM PVC ranges and is indexed by ifIndex, atmVclVpi, and rangeIndex. This table contains the following objects:
  - atmPVclLowerRangeValue
  - atmPVclHigherRangeValue
  - atmPVclRangeStatusChangeStart
  - atmPVclRangeStatusChangeEnd
- The ATM PVC Up Trap "atmIntfPvcUpTrap" contains the following objects:
  - ifIndex
  - atmIntfCurrentlyDownToUpPVcls
- The ATM PVC OAM Failure Trap "atmIntfPvcOAMFailureTrap" contains the following objects:

- ifIndex
- atmIntfOAMFailedPVcls
- atmIntfCurrentlyOAMFailingPVcls

How to Configure ATM SNMP Trap and OAM Enhancements

Configuring Extended ATM PVC Trap Support

Perform the following steps to configure extended ATM PVC trap support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps atm pvc extension** {**up**| **down**| **oam failure**[**aisrdi**| **endCC**| **loopback**| **segmentCC**]}
4. **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	**snmp-server enable traps atm pvc extension** {**up**| **down**| **oam failure**[**aisrdi**| **endCC**| **loopback**| **segmentCC**]} **Example:** `Router(config)# snmp-server enable traps atm pvc extension oam failure loopback`	Enables the sending of extended ATM PVC traps. The keywords are as follows: • **up** --Enables ATM PVC up traps that are generated when a PVC changes from the down to up state. • **down** --Enables ATM PVC failure traps that are generated when a PVC changes from the up to down state. • **oam failure** --Enables ATM PVC OAM failure traps that are generated when OAM failure occurs.

	Command or Action	Purpose
		• **aisrdi** --Enables AIS/RDI OAM failure traps that are generated when AIS/RDI OAM failure occurs. • **endCC** --Enables end-to-end OAM CC failure traps that are generated when end-to-end CC failures occur. • **loopback** --Enables OAM failure loopback traps that are generated when OAM loopback failure occurs. • **segmentCC** --Enables segment OAM CC failure traps that are generated when segment CC failures.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling OAM Management

When you configure PVC trap support, you must also enable OAM management on the PVC. Perform the following steps to enable OAM management.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot* **/0** [**.***subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   -
   - **interface atm** *slot* / *port-adapter* **/0** [**.***subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   -
   - **interface atm** interface-*number* [**.***subinterface-number* {**multipoint** | **point-to-point**}]
4. **pvc** [*name*]*vpi*/*vci*
5. **oam-pvc manage**
6. **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	Do one of the following: • **interface atm** *slot* **/0** [**.***subinterface-number* {**multipoint** | **point-to-point**}] • • • • **interface atm** *slot* / *port-adapter* **/0** [**.***subinterface-number* {**multipoint** | **point-to-point**}] • • • • **interface atm** interface-*number* [**.***subinterface-number* {**multipoint |** **point-to-point**}] **Example:** `Router(config)# interface atm 2/0`	Specifies the ATM interface using the appropriate form of the **interface atm** command.[22] The command syntax is as follows: • *interface-number* --Specifies a (physical) ATM interface (for example, 2/0). • **.** *subinterface-number* --Specifies a subinterface number. A dot (.) must be used to separate the interface-number from the subinterface-number (for example, 2/0.1). • **multipoint** --Specifies multipoint as the interface type for which a subinterface is to be created. • **point-to-point** --Specifies point-to-point as the interface type for which a subinterface is to be created.
Step 4	**pvc** [*name*]*vpi*/*vci* **Example:** `Router(config-if)# pvc oam 0/5`	Enables the PVC and enters ATM VC configuration mode.
Step 5	**oam-pvc manage** **Example:** `Router(config-if-atm-vc)# oam-pvc manage`	Enables end-to-end OAM management for an ATM PVC.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM VC configuration mode and returns to interface configuration mode.

[22] To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Enabling OAM AIS-RDI Monitoring

Perform the following task to enable OAM AIS-RDI Monitoring on VCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** interface-*number* [**.***subinterface-number* {**multipoint** | **point-to-point**}]
4. **pvc** [*name*] *vpi* / *vci*
5. **oam ais-rdi** [*down-count* [*up-count*]]
6. **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	**interface atm** interface-*number* [**.***subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 2/0`	Specifies the ATM interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 0/400`	Enables the PVC and enters ATM VC configuration mode.
Step 5	**oam ais-rdi** [*down-count* [*up-count*]] **Example:** `Router(config-if-atm-vc)# oam ais-rdi 1 3`	Configures an ATM PVC to be brought down after a specified number of OAM AIS/RDI cells have been received on the PVC or brought up if no OAM AIS/RDI cells have been received in a specified interval.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM VC configuration mode and returns to privileged EXEC mode.

Verifying ATM PVC Traps

To verify the configuration of ATM PVC traps, use the **show running-config** command. To view the status of ATM VCs, use the **show atm vc**command.

Following is an example of the **show atm vc** command:

```
Router# show atm vc
Codes: DN - DOWN, IN - INACTIVE
           VCD /                                              Peak Av/Min Burst
Interface  Name         VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
2/0        oam            0     5 PVC     SNAP       UBR       0              IN
2/0        7              0    10 PVC     SNAP       UBR       0              IN
2/0        2              0    40 PVC     SNAP       UBR       0              IN
2/0        1              0   100 PVC     SNAP       UBR       0              IN
2/0        name           1     1 PVC     SNAP       UBR       0              IN
2/0        4              2   200 PVC     SNAP       UBR       0              IN
2/0        vpi/vci        3   100 PVC     SNAP       UBR       0              IN
2/0        8              4   100 PVC     SNAP       UBR       0              IN
```

Configuration Examples for ATM SNMP Traps and OAM Enhancements

Configuring Extended ATM PVC Trap Support Example

The following example shows the three extended ATM PVC traps enabled on a router. If PVC 0/1 either leaves the up state, or down state, or encounters an OAM loopback failure, then the host 172.16.61.90 receives SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Extended ATM PVC Traps Output Examples

This section contains examples of output for the extended ATM PVC traps.

Extended ATM PVC Failure Trap Output

The following example shows the output for the extended ATM PVC failure trap for PVCs 1/100, 1/102, and 1/103. Note that only one trap is generated for all the PVCs associated with the same interface or subinterface (in contrast to the legacy ATM PVC failure trap that generates separate trap for each PVC). The VPI/VCI information and timing is located in the objects associated with the trap.

```
00:23:56:SNMP:Queuing packet to 1.1.1.1
00:23:56:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 143636
snmpTrapOID.0 = atmIntfPvcFailuresTrap
ifEntry.1.19 = 19
atmIntfPvcFailures.2 = 7
atmIntfCurrentlyFailingPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 140643
atmPVclRangeStatusChangeEnd.19.1.2 = 140698
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 140636
00:23:56:SNMP:Packet sent via UDP to 1.1.1.1
```

Extended ATM PVC Up Trap Output

The following example shows the output for the extended ATM PVC up trap for PVCs 1/100, 1/102, and 1/103:

```
00:31:29:SNMP:Queuing packet to 1.1.1.1
00:31:29:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 188990
snmpTrapOID.0 = atmIntfPvcUpTrap
ifEntry.1.19 = 19
atmIntfCurrentlyDownToUpPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 186005
atmPVclRangeStatusChangeEnd.19.1.2 = 186053
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 185990
atmPVclStatusChangeEnd.19.1.100 = 185990
```

Enabling OAM AIS-RDI Monitoring Example

The following example shows how to enable OAM ASI-RDI monitoring in ATM VC configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# interface atm 2/0
Router(config-if)# pvc 0/400
Router(config-if-atm-vc)# oam ais-rdi 25 5
Router(config-if-atm-vc)# end
```

The following example shows how to enable OAM ASI-RDI monitoring in ATM VC-Class configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm vctest
Router(config-vc-class)# oam ais-rdi 14 5
```

Router(config-if-atm-vc)# **end**

Additional References

Related Documents

Related Topic	Document Title
Configuring ATM	"Configuring ATM"
ATM commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples.	*Cisco IOS Asynchronous Transfer Mode Command Reference*
Configuring SNMP support	"Configuring SNMP Support"
SNMP commands	*Cisco IOS Network Management Command Reference*

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
• ATM PVC MIB • CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ATM SNMP Trap and OAM Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 12: Feature Information for ATM SNMP Trap and OAM Enhancements

Feature Name	Releases	Feature Information
ATM SNMP Trap and OAM Enhancements	12.2(4)T 12.2(4)T3	The feature provides enhancements to the Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) and to Operation, Administration, and Maintenance (OAM) functionality. In Cisco IOS Release 12.2.(4)T this feature was implemented on the Cisco 2600 series routers, the Cisco 3660 series routers and the Cisco 7200 series routers. The following sections provide information about this feature: The following commands were introduced or modified: **snmp-server enable traps atm pvc extension**, **oam-pvc manage**. In Release 12.2(4)T3, support was added for the Cisco 7500 series routers.

Feature Name	Releases	Feature Information
ATM OAM AIS-RDI Monitoring	15.0(1)M 12.0(28)S 12.2(33)SRE	The ATM OAM AIS-RDI Monitoring feature extends the existing ATM virtual circuit OAM functionality to include monitoring of the AIS-RDI. This feature was introduced in Cisco IOS Release 12.0(28)S. The following commands were introduced or modified: **oam ais-rdi**. This feature was integrated into Cisco IOS Release 12.2(33)SRE and Cisco IOS Release 15.0(1)M.

Glossary

inform --SNMP trap message that includes a delivery confirmation request.

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

NMS --Network Management System. An application or suite of applications designed to monitor networks using SNMP. CiscoView is one example of an NMS.

OAM --Operation, Administration, and Maintenance. ATM Forum specifies OAM cells used to monitor virtual circuits. OAM cells provide a virtual circuit-level loopback in which a router responds to the cells, demonstrating that the circuit is up and the router is operational.

PVC --Permanent Virtual Circuit. Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, PVC also stands for permanent virtual connection.

SNMP --Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents and is exclusively used in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

trap --A message from an SNMP agent alerting the SNMP manager to a condition on the network.

VCI --Virtual Channel Identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next network VCL that a cell needs to transit on its way to its final destination.

VCL --Virtual Channel Link. Connection between two ATM devices.

VPI --Virtual Path Identifier. Eight-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next VCL that a cell needs to transit on its way to its final destination. The function of the VPI is similar to that of the DLCI in Frame Relay.

CHAPTER 10

ATM SVC Troubleshooting Enhancements

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the ATM SVC Troubleshooting Enhancements feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

The ATM SVC Troubleshooting Enhancements feature introduces two new debug commands: **debug atm native** and **debug atm nmba**. These commands can be used to troubleshoot ATM switched virtual circuits (SVCs). The **debug atm nbma**and **debug atm native** commands are used to debug problems with Resource Reservation Protocol (RSVP) SVC creation and teardown. The **debug atm native**command can also be used to debug problems with SVCs created using static maps.

Benefits

The ATM SVC Troubleshooting Enhancements feature provides two debug commands that can be used to troubleshoot ATM SVCs that were created using static maps or RSVP.

Restrictions

The **debug atm nmba** command can be used only to debug RSVP SVCs. The **debug atm native** command can be used only to debug problems with RSVP SVCs or SVCs that were created using static maps.

Related Documents

- *Cisco IOS Wide-Area Networking Configuration Guide* , Release 12.2
- *Cisco IOS Wide-Area Networking Command Reference* , Release 12.2

Supported Platforms

- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7200 series
- Cisco 7500 series
- Cisco MC3810 series
- Universal Router Module (URM) for Cisco IGX 8400

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register .

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Supported Standards and MIBs and and RFCs

Standards

API Semantics for Native ATM Services , ATM Forum, February 1999

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

The tasks in this document assume that ATM SVCs or RSVP SVCs are already created.

Configuration Tasks

None.

Monitoring and Maintaining ATM SVCs

To monitor and maintain RSVP SVCs or ATM SVCs that were created using static maps, use the following commands in privileged EXEC mode:

Command	Purpose
`Router#` **debug atm native** {[**api**] | [**conn**] | [**error**] | [**filter**]}	Displays Native ATM API events.
`Router#` **debug atm nbma** [**api**]	Displays NBMA API events during the creation of RSVP SVCs.

Configuration Examples

None.

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Asynchronous Transfer Mode Command Reference*. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List*.

- **debug atm native**
- **debug atm nbma**

CHAPTER 11

ATM Software Segmentation and Reassembly

Feature History

Release	Modification
12.2(2)XB	Cisco 2600 Series T1/E1 ATM and Cisco 3660 T1 Inverse Multiplexing over ATM (IMA) ATM Adaption Layer 2 (AAL2) Support was introduced.
12.2(8)T	This feature was integrated into the Cisco IOS Release 12.2(8)T.

This document describes the ATM Software segmentation and reassembly (SAR) feature and includes the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

The ATM Software Segmentation and Reassembly (SAR) feature allows the Cisco 2600 series to carry voice and data traffic over ATM networks using AAL2 and AAL5 and allows the Cisco 3660 to support AAL2 voice traffic.

For the Cisco 2600 series, this feature works in conjunction with the T1/E1 multiflex voice/WAN interface card (VWIC), which is plugged into a WIC slot to provide one ATM WAN interface at a T1/E1 rate supporting up to 24/30 channels of voice.

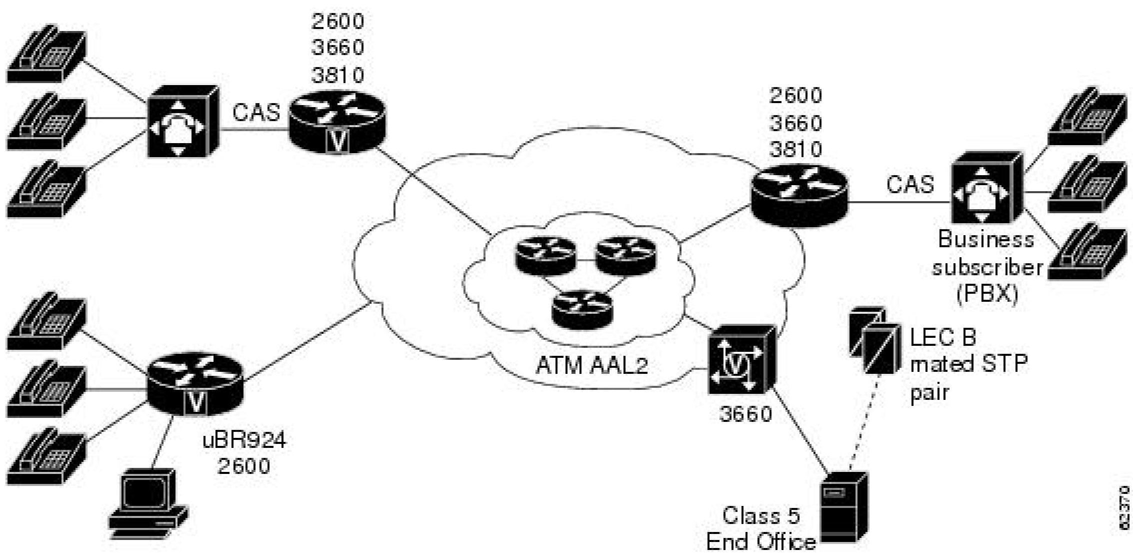
T1/E1 ATM support is a time-to-market feature that helps service providers take advantage of the inherent quality of service (QoS) features of ATM multiservice applications. FR-ATM (FRF.5 and FRF.8) internetworking is supported on the Cisco 2600 series.

On the Cisco 3660 a T1 IMA network module is used as the IMA interface providing a maximum of one ATM IMA interface that supports up to 48/60 voice channels. Up to eight T1/E1s and multiple IMA groups are permitted, but only the first IMA group supports voice over AAL2 for up to 48/60 voice channels. NM-IMA already supports AAL5 on both the Cisco 2600 series and Cisco 3600 series (not just 3660).

The Cisco 2600 Series T1/E1 ATM portion of this feature provides a shared implementation of the ATM features currently available on the Cisco MC3810 with the Cisco 2600 series.

The figure below illustrates the ATM AAL2 nonswitched trunking feature connecting two private branch exchanges (PBXs) together without the call agent (CA).

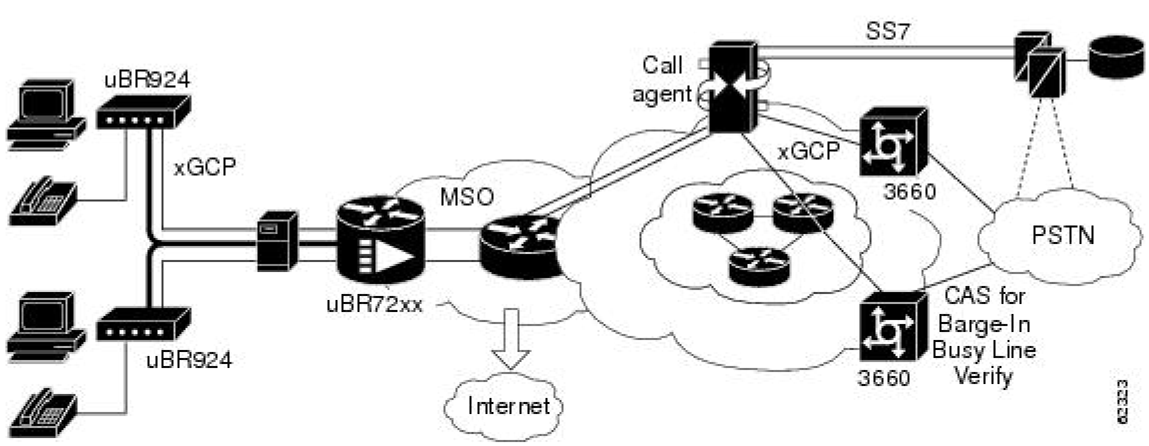
Figure 12: ATM AAL2 Non-Switched Trunking Solution



The next two figures below illustrate CA solutions. In these solutions, a CA provides business voice services traditionally offered by a circuit-based PBX.

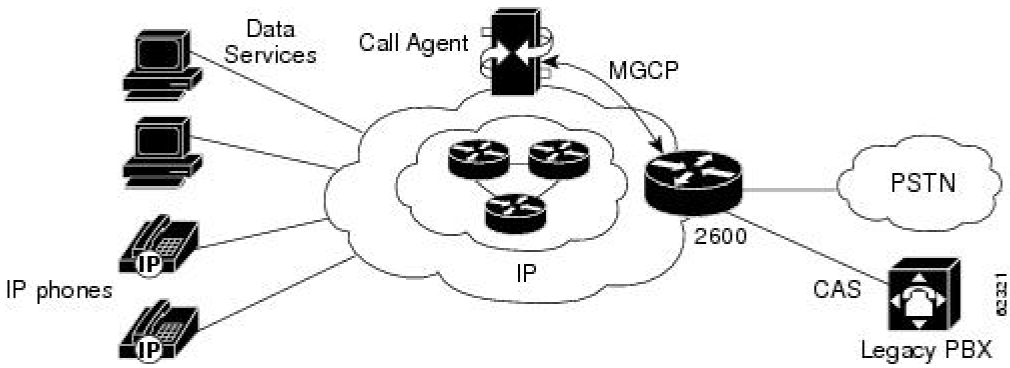
In the figure below, the trunking gateway (the Cisco 3660 platform) requires support of incoming and outgoing multi-frequency signaling for the barge-in and busy-line verify features. The residential gateway (the Cisco uBR924 cable access router) must support the CLASS features and 911 capability.

Figure 13: Residential Cable Access Solution



In the figure below, the gateway (the Cisco 2600 platform) requires PBX connectivity to interface with the legacy PBX.

Figure 14: IP Centrex Solution



Benefits

AAL2 and AAL5 Functionality

Adds AAL2 and AAL5 functionality to the Cisco 2600 series and AAL2 to the Cisco 3660 on an IMA network module. AAL2 and AAL5 are the most bandwidth-efficient, standards-based trunking methods for transporting compressed voice, voice-band data, and frame-mode data over ATM infrastructures.

Economical ATM SAR Option

Provides robust, low-cost addition of ATM software SAR functionality to the Cisco 2600 series.

Lower Overhead and Better QoS

Enhances continued use of existing ATM infrastructure, providing traditionally high ATM QoS.

Restrictions

Cisco 2600 Series and Cisco 3660

- Analog voice modules are not supported for AAL2 feature. (IP over ATM AAL5 is supported.)

Cisco 2600 Series

- SS7 and bisync protocol cannot be used when this feature is active.
- Only one T1/E1 multiflex VWIC is supported, setting the number of allowable T1/E1 ATM interfaces to one.
- Only the Cisco 2650 and Cisco 2651 support end-to-end, Network Traceable Reference (NTR) clocking. For the NTR clock to work correctly, the T1/E1 multiflex VWIC must be placed in slot zero of the Cisco

2650 and Cisco 2651. In the case where a two-port T1/E1 multiflex VWIC is installed in slot zero, either of the two ports can be configured for support, but only one can be supported.

- The T1/E1 ATM feature requires that the T1/E1 multiflex VWIC be placed in slot zero.

Cisco 3660

- Only one IMA group can support AAL2 voice. If there are multiple IMA groups, then only the first IMA group supports AAL2 voice.
- Two T1/E1s are supported for ATM and 48/60 voice ports for PBX.
- Only the T1/E1 IMA network module supports AAL2 voice. This feature does not support OC3/T3/E3 network modules.
- The T1/E1 IMA network module does not support an NTR clock.

Cisco 2620XM

- When the traffic is sent with rate 100pps (256 bytes size), some cells are lost on the router where VWIC-1MFT-E1 is configured as ATM port. There is no workaround to this limitation. For a detailed description, see Traffic Shaping on Cisco 3810 Routers at the following URL:

http://www.cisco.com/warp/public/121/traff_shape3810.pdf

Related Features and Technologies

- Media Gateway Control Protocol (MGCP) channel associated signaling (CAS) PBX and AAL2 permanent virtual circuit (PVC) Software
- PRI/Q.931 Signaling Backhaul
- Voice over ATM with AAL2 Trunking

Related Documents

- MGCP CAS PBX and AAL2 PVC
    - http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcptk.htm
- ATM forum documents for AAL2
    - ATM Trunking Using AAL2 for Narrowband Services (AF-VTOA-0113.000)

http://www.atmforum.com/atmforum/specs/approved.html

- ITU I-series documents located at

http://www.itu.int/home/index.html

-
    - I.363.2, *B-ISDN ATM Adaptation Layer Specification: Type 2 AAL*

- I.366.1, *Segmentation and Reassembly Service Specific Convergence Sublayer for the AAL Type 2*
- I.366.2, *AAL Type 2 Service Specific Convergence Sublayer for Trunking*

- Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2
- Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2
- Cisco IOS Interface Command Reference, Release 12.2
- Cisco IOS Interface Configuration Guide, Release 12.2

Supported Platforms

- Cisco 2600 series
- Cisco 3660

Supported Standards and MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

RFCs

- RFC 1577
- RFC 1483
- RFC 2221
- RFC 3661

Prerequisites

T1/E1 multiflex VWICs on Cisco 2600 series routers must be plugged into slot zero. The Cisco 3660 must be configured with a T1/E1 IMA Network Module. PBX voice requires a Digital T1/E1 Packet Voice Trunk Network Module Interface to be installed in the network module slot in the Cisco 2600 series or Cisco 3660.

You can configure the following four features on the Cisco 2600 series and Cisco 3660 routers:

- AAL2 Trunking with CAS
- AAL2 Trunking with common channel signaling (CCS)
- MGCP CAS
- MGCP Primary Rate Interface (PRI) Backhaul

Configuration Tasks for AAL2 Trunking with CAS

See the following sections for configuration tasks for AAL2 Trunking with CAS on Cisco 2600 series and Cisco 3660:

Configuring ATM on Cisco 2600 Series

This section describes the ATM configuration tasks necessary to support Voice over ATM using AAL2 on the Cisco 2600 series.

Note If any DS0 groups (CAS groups), channel groups, or clear channels are configured on T1/E1 controller 0, you must remove them before configuring VoATM. Because ATM uses all of the DS0 time slots on the controller, the ATM configuration cannot take place if any DS0s on controller 0 are used by other applications.

You must perform the VoATM configuration on the Cisco 2600 series or Cisco 3660 concentrators at both ends of the ATM link.

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

To configure a Cisco 2600 series or Cisco 3660 series concentrator to support VoATM on a T1/E1 trunk, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **controller t1 e1 0/0**
2. Router(config-controller)# **mode atm**
3. Router(config-controller)# framing *framing type*
4. Router(config-controller)# linecode *linecode type*
5. Router(config-controller)# **no shutdown**
6. Router(config-controller)# **exit**
7. Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]
8. Router(config-if)# **pvc***word*] { *vpi*/*vci* | *vci*
9. Router (config-if-atm-vc) # **encapsulation aal2**
10. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
11. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
12. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
13. Router(config-if-atm-vc)# **end**
14. Router# **show atm vc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller t1 e1 0/0**	Selects the T1 or E1 controller 0/0.
Step 2	Router(config-controller)# **mode atm** **Example:**	Specifies that the controller will support ATM encapsulation and create ATM interface 0/0.
Step 3	Router(config-controller)# framing *framing type*	Specifies the T1 framing type as extended superframe or **esf**. When the controller is set to ATM mode, the Controller framing is automatically set to Extended SuperFrame (**esf**) on T1 and to **crc4** on E1.
Step 4	Router(config-controller)# linecode *linecode type*	Specifies the T1 line code type as **b8zs**. The linecode is automatically set to b8zs on T1 and to HDB3 on E1.
Step 5	Router(config-controller)# **no shutdown**	Ensures that the controller is activated.
Step 6	Router(config-controller)# **exit**	Exits controller configuration mode.
Step 7	Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. For subinterfaces, the default is **multipoint**.
Step 8	Router(config-if)# **pvc***word*] { *vpi*/*vci* | *vci*	Creates an ATM PVC for voice traffic and enter ATM virtual circuit configuration mode.

	Command or Action	Purpose
		vpi= 0 to 255 vci= 1 to 1023 word= optional PVC identifier (letters only); if you assign a PVC identifier, you can use it to specify this PVC when configuring network dial peers **Note** AAL2 encapsulation is not supported for interim local management interface (ilmi) and Q signaling ATM adaption layer (qsaal) PVCs.
Step 9	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 10	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for variable-bit-rate real-time (VBRrt) (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • Peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • Average rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85 G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 20 byte sample size--max calls x 22 G.729 with 30 byte sample size--max calls x 15 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • Burst size--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 11	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specifies the number of seconds between loopback cells, and optionally enable operation, administration, and maintenance (OAM) management of the connection. The range for *frequency* is 0 to 600. The default is 10.
Step 12	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled.

	Command or Action	Purpose
		• The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 13	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 14	Router# **show atm vc**	Verifies the ATM PVC configuration.

Configuring ATM on Cisco 3660

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC, because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **interface atm <** *slot>/ima<grp#>* [*subinterface-number* [**multipoint** | **point-to-point**]]
2. Router(config-if)# pvc [*name*] *vpi/vci*
3. Router (config-if-atm-vc) # **encapsulation aal2**
4. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
5. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
6. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
7. Router(config-if-atm-vc)# **end**
8. Router# **show atm vc**
9. Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]
10. Router(config-if-atm-vc)# **vcci***pvc-identifier*
11. Router(config-if-atm-vc)# **exit**
12. Router(config-if)# **exit**
13. Router(config)# **dial-peer voice***number***pots**
14. Router(config-dial-peer)# **application MGCPAPP**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm <** *slot>/ima<grp#>* [*subinterface-number* [**multipoint** | **point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. **Note** To configure an IMA group on each ATM interface, enter the IMA group and group number. The default for subinterfaces is **multipoint.** *For all Scenarios* : Set up three subinterfaces for point-to-point.
Step 2	Router(config-if)# pvc [*name*] *vpi/vci*	Creates an ATM PVC for voice traffic and enters ATM virtual circuit configuration mode. **Note** AAL2 encap is not supported for ilmi and qsaal PVCs.
Step 3	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 4	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for VBR-rt (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • Peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • Average rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85

	Command or Action	Purpose
		G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 30 byte sample size--max calls x 15 G.729 with 20 byte sample size--max calls x 22 G.729 with 10 byte sample size--max calls x 43 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • Burst size--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 5	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specifies the number of seconds between loopback cells, and optionally enables OAM management of the connection. The range for *frequency* is 0 to 600. The default is 10.
Step 6	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled. • The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 7	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 8	Router# **show atm vc**	Verifies the ATM PVC configuration.
Step 9	Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]	Configure the PVC for the variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • Peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM).

	Command or Action	Purpose
		• Average rate--Calculate according to the maximum number of calls (max calls) the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: for VoIP: G.711 with 40 or 80 byte sample size: max calls x 128K G.726 with 40 byte sample size: max calls x 85K G.729a with 10 byte sample size: max calls x 85K for VoAAL2: G.711 with 40 byte sample size: max calls x 85K G.726 with 40 byte sample size: max calls x 43K G.729a with 10 byte sample size: max calls x 43K If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by a s much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • Burst size-- Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 10	Router(config-if-atm-vc)# **vcci***pvc-identifier*	Assigns a unique identifier to the PVC.
Step 11	Router(config-if-atm-vc)# **exit**	Exits ATM virtual circuit configuration mode.
Step 12	Router(config-if)# **exit**	Exits interface configuration mode.
Step 13	Router(config)# **dial-peer voice***number***pots**	Enters dial peer configuration mode for the plain old telephone service (POTS) dial peer.
Step 14	Router(config-dial-peer)# **application MGCPAPP**	Initiates the MGCP protocol for the voice ports.

Configuring Voice Band Detection Playout Settings

To configure voice band detection playout buffer delay on Cisco 2600 series and Cisco 3600 series routers , use the following commands beginning in the voice service configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# session protocol aal2
3. Router(config-voice-service-session)# vbd-playout-delay maximum time
4. Router(config-voice-service-session)# vbd-playout-delay minimum time
5. Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}
6. Router(config-voice-service-session)# vbd-playout-delay nominal time
7. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# session protocol aal2 **Example:**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# vbd-playout-delay maximum time	Specifies the maximum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers in milliseconds. The time is set in milliseconds. The range is from 40-1700 milliseconds. The default is set to 200 milliseconds.
Step 4	Router(config-voice-service-session)# vbd-playout-delay minimum time	Specifies the minimum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 4-1700 milliseconds. The default is set to 4 milliseconds.
Step 5	Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}	Configures voice band detection playout delay adaptation mode on a Cisco router. When the vbd-delay-playout mode is set to fixed, jitter buffer is set at a constant delay in milliseconds. When the vbd-delay-playout mode is set to passthrough, jitter buffer is set to DRAIN_FILL for clock compensation. There is no default.
Step 6	Router(config-voice-service-session)# vbd-playout-delay nominal time	Specifies the nominal AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 0-1500 milliseconds. The default is 100 milliseconds.
Step 7	Router(config-voice-service-session)# **end**	Exits voice-service-session configuration mode.

Configuring Subcell Multiplexing for AAL2 Voice

This section describes the configuration tasks necessary to enable AAL2 common part sublayer (CPS) subcell multiplexing when the Cisco 2600 series router or a Cisco 3660 interoperates with a voice interface service module (VISM) in an MGX switch.

To configure the Cisco 2600 series router or the Cisco 3660 to perform subcell multiplexing, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **subcell-mux <number>**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **subcell-mux <number>**	Enables subcell multiplexing. The number is time in milliseconds. By default, subcell multiplexing is not enabled.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring End-to-End Clocking

The following commands can be used to configure the Cisco 3660 only when there is a time-division multiplexing (TDM) switch module on board. For the Cisco 2600 series, these commands are automatically allowed.

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*
2. For Cisco 2600 series:
3. Router(config) **network-clock-select** *priority* **t1** *slot/port*
4. Router(config) **network-clock-select** *priority* **t1** *slot/port*
5. Router(config) **voice-card** *slot*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*	Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the VWIC by entering the keyword **wic** and the slot number 0 on the router.

Step 2	For Cisco 2600 series:
	Example:
	`Router(config)#` **network-clock-participate** {**nm** | **wic**} *slot*
	Example:
	Example:
	`For Cisco 3660:`
	Example:
	`Router(config)# network-clock-participate {nm} slot`
		Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the network module by entering the keyword **nm** and the slot number 1 on the router.

Step 3	Router(config) **network-clock-select** *priority* **t1** *slot/port*	Names a source to provide timing for the network clock and to specify the selection *priority* for this clock source. The priority selection is *1* or *2* . Use the **no** form of this command to cancel the selection.
Step 4	Router(config) **network-clock-select** *priority* **t1** *slot/port*	Assigns *priority 1* to ATM interface 0/0 and *priority 2* to controller 1/0.
Step 5	Router(config) **voice-card** *slot*	Enters voice-card configuration mode and sets codec complexity. For *slot,* use a value from 0 to 3 that describes the card location in the module.

Configuring a CAC Master for AAL2 Voice

This section describes the configuration tasks necessary to configure call admission control (CAC) for AAL2 voice. The commands and procedures in this section are common to the Cisco 2600 series and the Cisco 3660 routers.

You can configure a Cisco 2600 series router or a Cisco 3660 as either a CAC master or a CAC slave. By default, this is a CAC slave. You typically configure a CAC master at one end of an ATM trunk and a CAC slave at the opposite end. A Cisco 2600 series router or a Cisco 3660 configured as a master always performs CAC during fax/modem upspeed. A Cisco 2600 series router or a Cisco 3660 configured as a slave sends a request for CAC to the CAC master.

To configure a Cisco 2600 series router or a Cisco 3660 as a CAC master, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC master.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring a CAC Slave for AAL2 Voice

To return a Cisco 2600 series router or a Cisco 3660 to its default operation as a CAC slave, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **no cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **no cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC slave.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring Dial Peers for AAL2 Voice

For more information on dial peers and dial-peer configuration, see the "Configuring Voice over ATM" chapter in the Cisco IOS *Multiservice Applications Configuration Guide,* Release 12.1.

Configuring Network Dial Peers to Support AAL2

To configure a network dial peer for Voice over ATM (VoATM), specify a unique tag number, an ATM, a virtual circuit number, and a channel identifier (CID).

To configure VoATM dial peers, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **dial-peer voice***tag* **voatm**
2. Router(config-dial-peer)# **destination-pattern** *string*
3. Router(config-dial-peer)# **session protocol aal2-trunk**
4. Router(config-dial-peer)# **session target atm 0/0 pvc** *word* | *vpi/vci* | *vci* } *cid*
5. Router(config-dial-peer)# **codec aal2 profile itut** |**custom** *profile-number codec*
6. Router(config-dial-peer)# **dtmf-relay**
7. Router(config-dial-peer)# **signal-type ext-signal transparent**
8. Router(config-dial-peer)# **no vad**
9. Router(config-dial-peer)# **exit**
10. **Repeat Step 1 through Step 9**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **dial-peer voice***tag* **voatm**	Defines a VoATM dial peer for VoATM and enters dial-peer configuration mode. The *tag* identifies the dial peer. Each *tag* on any one router must be unique.
Step 2	Router(config-dial-peer)# **destination-pattern** *string*	Configures the dial peer's destination pattern. The *string* is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9 and the letters A through D. The following special characters can be entered in the string: • The star (*) and the pound sign (#) can be used in a dial string, but not as leading characters (for example *650 is not permitted). • The period (.) can be entered as a wildcard digit. Network dial peers typically use wildcards to represent a range of destination telephone numbers (for example, 1408555.... for all numbers in area code 408 with the 555 prefix). • The comma (,) can be used only in prefixes, and is used to insert a 1-second pause. • The timer (T) character can be used to configure variable-length dial plans.
Step 3	Router(config-dial-peer)# **session protocol aal2-trunk**	Configures the session protocol to support AAL2-trunk permanent (private line) trunk calls.
Step 4	Router(config-dial-peer)# **session target atm 0/0 pvc** *word* | *vpi/vci* | *vci* } *cid* **Example:** `(for Cisco 2600 series)`	Configures the ATM session target for the dial peer. Be sure to specify **atm 0/0** as the interface for the PVC. Use *word* to identify the PVC if a word name was assigned when the PVC was created in the Configuring ATM on Cisco 2600 Series, on page 241. Use *word* to identify the PVC if a word name was assigned when the PVC was created in the Configuring ATM on Cisco 3660, on page 244.

	Command or Action	Purpose
	Example: `For Cisco 3660:` **Example:** `router(config-dial-peer)#` **session target atm <slot>/ima <group#>**	
Step 5	Router(config-dial-peer)# **codec aal2 profile itut |custom** *profile-number codec*	Specifies a codec profile for the DSP. Profile options are **itut 1**, **itut 2**, **itut 7**, **custom 100**, and **custom 110**. The default is **itut 1** with codec G.711 u-law. See the "Command Reference" section for the codec options available for each AAL2 profile. **Note** Use this command instead of the **codec (dial-peer)**command for AAL2 trunk applications.
Step 6	Router(config-dial-peer)# **dtmf-relay**	(Optional) If the **codec** type is a low bit-rate codec such as **g729** or **g723**, specify support for dual tone multifrequency (DTMF) relay to improve end-to-end transport of DTMF tones. DTMF tones do not always propagate reliably with low bit-rate codecs. DTMF relay is disabled by default.
Step 7	Router(config-dial-peer)# **signal-type ext-signal transparent**	(Optional) Defines the type of ABCD signaling packets that are generated by the voice port and sent over the ATM network. The signal type must be configured to the same setting at both ends of the PVC. Enter **ext-signal** for common channel signaling (CCS). ABCD signaling packets are not sent. Enter **transparent** for nonswitched trunks using channel associated signaling (CAS). ABCD signaling bits are passed transparently to the ATM network.
Step 8	Router(config-dial-peer)# **no vad**	(Optional) Disables voice activity detection (VAD) on the dial peer. VAD is enabled by default.
Step 9	Router(config-dial-peer)# **exit**	Exits from the dial-peer configuration mode.
Step 10	**Repeat Step 1 through Step 9**	Configures additional VoATM dial peers.

What to Do Next

Configuring MGCP POTS Dial Peer

To configure MGCP POTS dial peer on the Cisco 2600 series and Cisco 3660, complete the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# dial-peer voice number pots
2. Router(config-dial-peer)# application MGCPAPP
3.
4. Router(config-dial-peer)# exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# dial-peer voice number pots	Enters the dial-peer configuration mode for the POTS dial peer.
Step 2	Router(config-dial-peer)# application MGCPAPP	Initiates the MGCP protocol for the voice ports.
Step 3	**Example:** `Router(config-dial-peer)# port slot/port:ds0-group`	This command associates the dial peer with a specific logical interface. The value of slot is the router location where the voice port adapter is installed. Valid entries are from 0 to 3. The value of port indicates the voice interface card location. Valid entries are 0 or 1. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
Step 4	Router(config-dial-peer)# exit	Exits from the dial-peer configuration mode.

Configuring DS-0 group for CAS

To configure ds0 group for CAS on the Cisco 2600 series and Cisco 3660, complete the following steps:

SUMMARY STEPS

1. Router(config)# **controller**{**t1** | **e1**} *slot/port*
2. Router(config-controller)# **mode cas**
3. Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type*
4. Router(config-controller)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller**{**t1** | **e1**} *slot/port*	*For the CAS PBX Scenarios only* : Selects the T1/E1 controller 1/0.
Step 2	Router(config-controller)# **mode cas**	*For the CAS PBX Scenarios only* : Specifies that the controller will support CAS.
Step 3	Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type*	*For the CAS PBX Scenarios only* : Configures the T1 time slots for CAS calls. The scenarios use the following three DS0 definitions: • ds0-group 1 time slots 1-8 type e&m-immediate-start • ds0-group 2 time slots 9-16 type e&m-wink-start • ds0-group 3 time slots 17-24 type fxs-ground-start
Step 4	Router(config-controller)# **exit**	*For the CAS PBX Scenarios only* : Exits controller configuration mode.

Configuration Tasks for AAL2 Trunking with CCS

See the following sections for configuration tasks for AAL2 Trunking with CCS on Cisco 2600 series and Cisco 3660:

Configuring ATM on the Cisco 2600 Series

This section describes the ATM configuration tasks necessary to support Voice over ATM using AAL2 on Cisco 2600 series.

Note If any DS0 groups (CAS groups), channel groups, or clear channels are configured on T1/E1 controller 0, you must remove them before configuring VoATM. Because ATM uses all of the DS0 time slots on the controller, the ATM configuration cannot take place if any DS0s on controller 0 are used by other applications.

You must perform the VoATM configuration on the Cisco 2600 series or Cisco 3660 concentrators at both ends of the ATM link.

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC, because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

To configure a Cisco 2600 series or Cisco 3660 series concentrator to support VoATM on a T1/E1 trunk, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **controller t1 e1 0/0**
2. Router(config-controller)# **mode atm**
3. Router(config-controller)# framing *framing type*
4. Router(config-controller)# linecode *linecode type*
5. Router(config-controller)# **no shutdown**
6. Router(config-controller)# **exit**
7. Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]
8. Router(config-if)# **pvc***word*] { *vpi/vci* | *vci*
9. Router (config-if-atm-vc) # **encapsulation aal2**
10. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
11. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
12. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
13. Router(config-if-atm-vc)# **end**
14. Router# **show atm vc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller t1 e1 0/0**	Selects the T1 or E1 controller 0/0.
Step 2	Router(config-controller)# **mode atm** **Example:**	Specifies that the controller will support ATM encapsulation and create ATM interface 0/0.
Step 3	Router(config-controller)# framing *framing type*	Specifies the T1 framing type as extended super frame or **esf**. When the controller is set to ATM mode, the Controller framing is automatically set to Extended SuperFrame (esf) on T1 and to crc4 on E1.
Step 4	Router(config-controller)# linecode *linecode type*	Specifies the T1 linecode type as **b8zs**. The linecode is automatically set to b8zs on T1 and to hdb3 on E1.
Step 5	Router(config-controller)# **no shutdown**	Ensures that the controller is activated.
Step 6	Router(config-controller)# **exit**	Exits controller configuration mode.
Step 7	Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. For subinterfaces, the default is **multipoint**.
Step 8	Router(config-if)# **pvc***word*] { *vpi/vci* | *vci*	Creates an ATM PVC for voice traffic and enters ATM virtual circuit configuration mode.

	Command or Action	Purpose
		vpi= 0 to 255 vci= 1 to 1023 word= optional PVC identifier (letters only); if you assign a PVC identifier, you can use it to specify this PVC when configuring network dial peers **Note** AAL2 encap is not supported for ilmi and qsaal PVCs.
Step 9	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 10	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak-rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average-rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85 G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 30 byte sample size--max calls x 15 G.729 with 20 byte sample size--max calls x 22 G.729 with 30 byte sample size--max calls x 15 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 11	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specifies the number of seconds between loopback cells, and optionally enables OAM management of the connection. The range for *frequency* is 0 to 600. The default is 10.

	Command or Action	Purpose
Step 12	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled. • The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 13	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 14	Router# **show atm vc**	Verifies the ATM PVC configuration.

Configuring ATM on the Cisco 3660

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **interface atm <** *slot>/ima<grp#>* [*subinterface-number* [**multipoint** | **point-to-point**]]
2. Router(config-if)# pvc [*name*] *vpi/vci*
3. Router (config-if-atm-vc) # **encapsulation aal2**
4. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
5. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
6. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
7. Router(config-if-atm-vc)# **end**
8. Router# **show atm vc**
9. Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]
10. Router(config-if-atm-vc)# **vcci***pvc-identifier*
11. Router(config-if-atm-vc)# **exit**
12. Router(config-if)# **exit**
13. Router(config)# **dial-peer voice***number***pots**
14. Router(config-dial-peer)# **application MGCPAPP**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm <** *slot>/ima<grp#>* [*subinterface-number* [**multipoint** | **point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. **Note** To configure an IMA group on each ATM interface, enter the IMA group and group number. The default for subinterfaces is **multipoint.** *For all Scenarios* : Set up three subinterfaces for point-to-point.
Step 2	Router(config-if)# pvc [*name*] *vpi/vci*	Creates an ATM PVC for voice traffic and enters ATM virtual circuit configuration mode. **Note** AAL2 encap is not supported for ilmi and qsaal PVCs.
Step 3	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 4	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85

	Command or Action	Purpose
		G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 30 byte sample size--max calls x 15 G.729 with 20 byte sample size--max calls x 22 G.729 with 10 byte sample size--max calls x 43 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst size--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 5	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specify the number of seconds between loopback cells, and optionally enable OAM management of the connection. The range for *frequency* is 0 to 600. The default is 10.
Step 6	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled. • The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 7	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 8	Router# **show atm vc**	Verifies the ATM PVC configuration.
Step 9	Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]	Configures the PVC for the variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM).

	Command or Action	Purpose
		• average rate--Calculate according to the maximum number of calls (max calls) the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: for VoIP: G.711 with 40 or 80 byte sample size: max calls x 128K G.726 with 40 byte sample size: max calls x 85K G.729a with 10 byte sample size: max calls x 85K for VoAAL2: G.711 with 40 byte sample size: max calls x 85K G.726 with 40 byte sample size: max calls x 43K G.729a with 10 byte sample size: max calls x 43K If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by a s much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 10	Router(config-if-atm-vc)# **vcci***pvc-identifier*	Assigns a unique identifier to the PVC.
Step 11	Router(config-if-atm-vc)# **exit**	Exits ATM virtual circuit configuration mode.
Step 12	Router(config-if)# **exit**	Exits interface configuration mode.
Step 13	Router(config)# **dial-peer voice***number***pots**	Enter dial peer configuration mode for the POTS dial peer.
Step 14	Router(config-dial-peer)# **application MGCPAPP**	Initiates the MGCP protocol for the voice ports.

Configuring Voice Band Detection Playout Settings

To configure voice band detection playout buffer delay on Cisco 2600 series and Cisco 3600 series routers , use the following commands beginning in the voice service configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# session protocol aal2
3. Router(config-voice-service-session)# vbd-playout-delay maximum time
4. Router(config-voice-service-session)# vbd-playout-delay minimum time
5. Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}
6. Router(config-voice-service-session)# vbd-playout-delay nominal time
7. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# session protocol aal2 **Example:**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# vbd-playout-delay maximum time	Specifies the maximum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers in milliseconds. The time is set in milliseconds. The range is from 40-1700 milliseconds. The default is set to 200 milliseconds.
Step 4	Router(config-voice-service-session)# vbd-playout-delay minimum time	Specifies the minimum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 4-1700 milliseconds. The default is set to 4 milliseconds.
Step 5	Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}	Configures voice band detection playout delay adaptation mode on a Cisco router. When the vbd-delay-playout mode is set to fixed, jitter buffer is set at a constant delay in milliseconds. When the vbd-delay-playout mode is set to passthrough, jitter buffer is set to DRAIN_FILL for clock compensation. There is no default.
Step 6	Router(config-voice-service-session)# vbd-playout-delay nominal time	Specifies the nominal AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 0-1500 milliseconds. The default is 100 milliseconds.
Step 7	Router(config-voice-service-session)# **end**	Exits voice-service-session configuration mode.

Configuring Subcell Multiplexing for AAL2 Voice

This section describes the configuration tasks necessary to enable AAL2 common part sublayer (CPS) subcell multiplexing when the Cisco 2600 series router or a Cisco 3660 interoperates with a voice interface service module (VISM) in an MGX switch.

To configure the Cisco 2600 series router or the Cisco 3660 to perform subcell multiplexing, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **subcell-mux <number>**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **subcell-mux <number>**	Enables subcell multiplexing. The number is time in milliseconds. By default, subcell multiplexing is not enabled.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring End-to-End Clocking

The following commands can be used to configure the Cisco3660 only when there is a TDM switch module on board. For Cisco 2600 series these commands are automatically allowed.

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*
2. For Cisco 2600 series:
3. Router(config) **network-clock-select** *priority* **t1** *slot/port*
4. Router(config) **network-clock-select** *priority* **t1** *slot/port*
5. Router(config) **voice-card** *slot*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*	Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the VWIC by entering the keyword **wic** and the slot number 0 on the router.

Step 2	For Cisco 2600 series:
	Example:
	`Router(config)#` **network-clock-participate** {**nm** | **wic**} *slot*
	Example:
	Example:
	`For Cisco 3660:`
	Example:
	`Router(config)# network-clock-participate {nm} slot`
		Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the network module by entering the keyword **nm** and the slot number 1 on the router.

Step 3	Router(config) **network-clock-select** *priority* **t1** *slot/port*	Names a source to provide timing for the network clock and to specify the selection *priority* for this clock source. The priority selection is *1* or *2* . Use the **no** form of this command to cancel the selection.
Step 4	Router(config) **network-clock-select** *priority* **t1** *slot/port*	Assigns *priority 1* to ATM interface 0/0 and *priority 2* to controller 1/0
Step 5	Router(config) **voice-card** *slot*	Enters voice-card configuration mode and set codec complexity. For *slot* use a value from 0 to 3 that describes the card location in the module.

Configuring a CAC Master for AAL2 Voice

This section describes the configuration tasks necessary to configure call admission control (CAC) for AAL2 voice. The commands and procedures in this section are common to the Cisco 2600 series and the Cisco 3660.

You can configure a Cisco 2600 series router or a Cisco 3660 as either a CAC master or a CAC slave. By default, this is a CAC slave. You typically configure a CAC master at one end of an ATM trunk and a CAC slave at the opposite end. A Cisco 2600 series router or a Cisco 3660 configured as a master always performs CAC during fax/modem upspeed. A Cisco 2600 series router or a Cisco 3660 configured as a slave sends a request for CAC to the CAC master.

To configure a Cisco 2600 series router or a Cisco 3660 as a CAC master, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC master.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring a CAC Slave for AAL2 Voice

To return a Cisco 2600 series router or a Cisco 3660 to its default operation as a CAC slave, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **no cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **no cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC slave.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring Dial Peers for AAL2 Voice

For more information on dial peers and dial-peer configuration, see the "Configuring Voice over ATM" chapter in the Cisco IOS *Multiservice Applications Configuration Guide,* Release 12.1.

Configuring Network Dial Peers to Support AAL2

To configure a network dial peer for Voice over ATM (VoATM), specify a unique tag number, an atm, a virtual circuit number, and channel identifier (CID).

To configure VoATM dial peers, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **dial-peer voice***tag* **voatm**
2. Router(config-dial-peer)# **destination-pattern** *string*
3. Router(config-dial-peer)# **session protocol aal2-trunk**
4. Router(config-dial-peer)# **session target atm 0/0 pvc** *word* | *vpi*/*vci* | *vci* } *cid*
5. Router(config-dial-peer)# **codec aal2 profile itut** |**custom** *profile-number codec*
6. Router(config-dial-peer)# **dtmf-relay**
7. Router(config-dial-peer)# **signal-type ext-signal transparent**
8. Router(config-dial-peer)# **no vad**
9. Router(config-dial-peer)# **exit**
10. **Repeat Step 1 through Step 9**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **dial-peer voice***tag* **voatm**	Defines a VoATM dial peer for VoATM and enter dial-peer configuration mode.

	Command or Action	Purpose
		The *tag* identifies the dial peer. Each *tag* on any one router must be unique.
Step 2	Router(config-dial-peer)# **destination-pattern** *string*	Configures the dial peer's destination pattern. The *string* is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9 and the letters A through D. The following special characters can be entered in the string: • The star (*) and the pound sign (#) can be used in a dial string, but not as leading characters (for example *650 is not permitted). • The period (.) can be entered as a wildcard digit. Network dial peers typically use wildcards to represent a range of destination telephone numbers (for example, 1408555.... for all numbers in area code 408 with the 555 prefix). • The comma (,) can be used only in prefixes, and is used to insert a 1-second pause. • The timer (T) character can be used to configure variable-length dial plans.
Step 3	Router(config-dial-peer)# **session protocol aal2-trunk**	Configures the session protocol to support AAL2-trunk permanent (private line) trunk calls.

Step 4	Router(config-dial-peer)# **session target atm 0/0 pvc** *word* | *vpi/vci* | *vci* } *cid*
	Example:
	`(for Cisco 2600 series)`
	Example:
	`For Cisco 3660:`
	Example:
	`router(config-dial-peer)#` **session target atm <slot>/ima <group#>**
		Configures the ATM session target for the dial peer. Be sure to specify **atm 0/0** as the interface for the PVC.
		Use *word* to identify the PVC if a word name was assigned when the PVC was created in the Configuring ATM on Cisco 2600 Series, on page 241.
		Use *word* to identify the PVC if a word name was assigned when the PVC was created in the Configuring ATM on Cisco 3660, on page 244.

Step 5	Router(config-dial-peer)# **codec aal2 profile itut** |**custom** *profile-number codec*	Specifies a codec profile for the DSP. Profile options are **itut 1**, **itut 2**, **itut 7**, **custom 100**, and **custom 110**. The default is **itut 1** with codec G.711 u-law. See the "Command Reference" section for the codec options available for each AAL2 profile. **Note** Use this command instead of the **codec (dial-peer)**command for AAL2 trunk applications.

	Command or Action	Purpose
Step 6	Router(config-dial-peer)# **dtmf-relay**	(Optional) If the **codec** type is a low bit-rate codec such as **g729** or **g723**, specify support for DTMF relay to improve end-to-end transport of DTMF tones. DTMF tones do not always propagate reliably with low bit-rate codecs. DTMF relay is disabled by default.
Step 7	Router(config-dial-peer)# **signal-type ext-signal transparent**	(Optional) Defines the type of ABCD signaling packets that are generated by the voice port and sent over the ATM network. The signal type must be configured to the same setting at both ends of the PVC. Enter **ext-signal** for common channel signaling (CCS). ABCD signaling packets are not sent. Enter **transparent** for nonswitched trunks using channel associated signaling (CAS). ABCD signaling bits are passed transparently to the ATM network.
Step 8	Router(config-dial-peer)# **no vad**	(Optional) Disables voice activity detection (VAD) on the dial peer. VAD is enabled by default.
Step 9	Router(config-dial-peer)# **exit**	Exits from the dial-peer configuration mode.
Step 10	**Repeat Step 1 through Step 9**	Configures additional VoATM dial peers.

Configuring MGCP POTS Dial Peer

To configure MGCP POTS dial peer on the Cisco 2600 series and the Cisco 3660, complete the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# dial-peer voice number pots
2. Router(config-dial-peer)# application MGCPAPP
3.
4. Router(config-dial-peer)# exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# dial-peer voice number pots	Enters the dial-peer configuration mode for the POTS dial-peer.
Step 2	Router(config-dial-peer)# application MGCPAPP	Initiates the MGCP protocol for the voice ports.

	Command or Action	Purpose
Step 3	**Example:** `Router(config-dial-peer)# port slot/port:ds0-group`	This command associates the dial peer with a specific logical interface. The value of slot is the router location where the voice port adapter is installed. Valid entries are from 0 to 3. The value of port indicates the voice interface card location. Valid entries are 0 or 1. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
Step 4	Router(config-dial-peer)# exit	Exits from the dial-peer configuration mode.

Configuring DS-0 Group and Channel Group for CCS

To configure a DS-0 group and the channel group for CCS on the Cisco 2600 series and the Cisco 3660, complete the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# controller {T1 | E1} slot/port
2. Router(config-controller)# mode ccs frame-forwarding
3. Router(config-controller)# channel-group number timeslots range speed{48|56|64}]
4. Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type*
5. Router(config-controller)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# controller {T1 | E1} slot/port	Enters controller configuration mode for the controller at the specified slot/port location. Valid values for slot and port are 0 and 1.
Step 2	Router(config-controller)# mode ccs frame-forwarding	Configures the controller to support CCS transparent signaling.
Step 3	Router(config-controller)# channel-group number timeslots range speed{48|56|64}]	Defines the time slots that belong to each T1 or E1 circuit. • number--channel-group number. When configuring a T1 data line, channel-group numbers can be values from 0 to 23. When configuring an E1 data line, channel-group numbers can be a values from 0 to 30. • range--time slot or range of time slots belonging to the channel group. The first timeslot is numbered 1. Pick one timeslot from the timeslot range. For a T1 controller, the timeslot range is from 1 to 24. For an E1 controller, the timeslot range is from 1 to 31.

	Command or Action	Purpose
		• speed {48 | 56 | 64}--(Optional) Specifies the line speed (in kilobits per second) of the T1 or E1 link. The default line speed for T1 is 56 kbps. The default line speed for E1 is 64 kbps.
Step 4	Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type*	*For the CCS PBX Scenarios only* : Configures the T1 time slots for CCS calls. The signaling type is external signaling.
Step 5	Router(config-controller)# **exit**	*For the CCS PBX Scenarios only* : Exits controller configuration mode.

Configuring T-CCS Frame Forwarding

To configure T-CCS frame-forwarding on the Cisco 2600 series and the Cisco 3660, complete the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# interface serial 1:channelnumber
2. Router(config-if)# ccs encap atm
3. Router(config-if)# ccs connect {serial |atm} slot/number [dlci dlci| pvc vci | pvc vcd | pvc vpi/vci | pvc string]
4. Router(config-if)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# interface serial 1:channelnumber	Enters interface configuration mode. This procedure maps the D channel from the digital T1/E1 packet voice trunk network module to the specified interface. The channel number argument specifies the channel number. For T1, enter the channel number as 23. For E1, enter 15.
Step 2	Router(config-if)# ccs encap atm	(ATM only) Configures the CCS encapsulation to use the ATM packet format.
Step 3	Router(config-if)# ccs connect {serial |atm} slot/number [dlci dlci| pvc vci | pvc vcd | pvc vpi/vci | pvc string]	(Frame Relay and ATM) Configures the CCS connection. If the CCS connection is over Frame Relay, specify a serial interface and the DLCI. If the CCS connection is over ATM, specify ATM, slot and interface, and the PVC.
Step 4	Router(config-if)# **exit**	Exits the interface mode.

Configuration Tasks for MGCP CAS

See the following sections for configuration tasks for MGCP CAS on Cisco 2600 series and Cisco 3660 routers. Each task in this list is identified as either required or optional:

Configuring MGCP CAS PBX on the Cisco 2600 Series and Cisco 3660

Use the following commands for configuring the Media Gateway Control Protocol (MGCP) CAS PBX on Cisco 2600 series and Cisco 3660 routers:

SUMMARY STEPS

1. Router(config)# **mgcp**
2. Router(config)# **mgcp call-agent** *ipaddr* | *hostname*} [*port*] [**service-type** *type*] **version** *version-number*
3. Router(config-if)# **mgcp sgcp restart notify**
4. Router(config-if)# **mgcp modem passthrough [cisco | ca | nse]**
5. Router(config)# **mgcp tse payload***type*
6. Router(config)# **no mgcp timer receive-rtcp**
7. Router(config)# **mgcp timer rtp-nse***timer*
8. Router(config)# **mgcp quarantine mode process**
9. Router(config)# **controller**{**t1** | **e1**} *slot/port*
10. Router(config-controller)# **mode cas**
11. Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type* **tone** *type* **addr info service** *service-type*
12. Router(config-controller)# **exit**
13. Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]
14. Router(config-if-atm-vc)# **vcci***pvc-identifier*
15. Router(config-if-atm-vc)# **exit**
16. Router(config-if)# **exit**
17. Router(config)# **dial-peer voice***number***pots**
18. Router(config-dial-peer)# **application MGCPAPP**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **mgcp**	Starts the MGCP daemon.
Step 2	Router(config)# **mgcp call-agent** *ipaddr* | *hostname*} [*port*] [**service-type** *type*] **version** *version-number*	Configures the MGCP call agent and service type.

	Command or Action	Purpose
Step 3	Router(config-if)# **mgcp sgcp restart notify**	Causes MGCP to send and process simple gateway control protocol (SGCP) restart in progress (RSIP) messages.
Step 4	Router(config-if)# **mgcp modem passthrough [cisco | ca | nse]**	Enables the router to process fax or modem messages. VoAAL2 does not support cisco.
Step 5	Router(config)# **mgcp tse payload***type*	Enables the telephony signaling events (TSE) payload for fax and modem messages.
Step 6	Router(config)# **no mgcp timer receive-rtcp**	Turns off the real-time transport protocol (RTP) RTP control protocol (RTCP) transmission interval at the gateway.
Step 7	Router(config)# **mgcp timer rtp-nse***timer*	Turns on the RTP named signaling events (NSE) timeout interval at the gateway.
Step 8	Router(config)# **mgcp quarantine mode process**	(Optional) Turns on processing for MGCP quarantine mode.
Step 9	Router(config)# **controller**{**t1** | **e1**} *slot/port*	*For the CAS PBX scenarios only* : Selects the T1/E1 controller 1/0.
Step 10	Router(config-controller)# **mode cas**	*For the CAS PBX scenarios only* : Specifies that the controller will support CAS.
Step 11	Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type* **tone** *type* **addr info service** *service-type*	*For the CAS PBX scenarios only* : Configures the T1 time slots for CAS calls. The scenarios use the following three digital signal level 0 (DS-0) definitions: • ds0-group 1 time slots 1-8 type e&m-immediate-start • ds0-group 2 time slots 9-16 type e&m-wink-start • ds0-group 3 time slots 17-24 type fxs-ground-start
Step 12	Router(config-controller)# **exit**	*For the CAS PBX scenarios only* : Exits controller configuration mode.
Step 13	Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]	Configure the PVC for the variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: For VoIP: G.711 with 169 or 80 byte sample size: max calls x 128K G.726 with 40 byte sample size: max calls x 85K G.729a with 10 byte sample size: max calls x 85K For VoAAL2:

	Command or Action	Purpose
		G.711 with 40 byte sample size: max calls x 85K G.726 with 40 byte sample size: max calls x 43K G.729a with 30 byte sample size: max calls x 15K If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst-- Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 times the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 14	Router(config-if-atm-vc)# **vcci***pvc-identifier*	Assigns a unique identifier to the PVC.
Step 15	Router(config-if-atm-vc)# **exit**	Exits ATM virtual circuit configuration mode.
Step 16	Router(config-if)# **exit**	Exits interface configuration mode.
Step 17	Router(config)# **dial-peer voice***number***pots**	Enters dial-peer configuration mode for the POTS dial peer.
Step 18	Router(config-dial-peer)# **application MGCPAPP**	Initiates MGCP for the voice ports. You can enter the MGCPAPP keyword in either uppercase or lowercase.

Configuring ATM on the Cisco 2600 Series

This section describes the ATM configuration tasks necessary to support Voice over ATM using AAL2 on Cisco 2600 series.

Note If any DS0 groups (CAS groups), channel groups, or clear channels are configured on T1/E1 controller 0, you must remove them before configuring VoATM. Because ATM uses all the DS-0 time slots on the controller, the ATM configuration cannot take place if any DS0s on controller 0 are used by other applications.

You must perform the VoATM configuration on the Cisco 2600 series or Cisco 3660 concentrators at both ends of the ATM link.

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC, because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

To configure a Cisco 2600 series or Cisco 3660 series concentrator to support VoATM on a T1/E1 trunk, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **controller t1 e1 0/0**
2. Router(config-controller)# **mode atm**
3. Router(config-controller)# framing *framing type*
4. Router(config-controller)# linecode *linecode type*
5. Router(config-controller)# **no shutdown**
6. Router(config-controller)# **exit**
7. Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]
8. Router(config-if)# **pvc***word*] { *vpi*/*vci* | *vci*
9. Router (config-if-atm-vc) # **encapsulation aal2**
10. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
11. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
12. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
13. Router(config-if-atm-vc)# **end**
14. Router# **show atm vc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller t1 e1 0/0**	Selects the T1 or E1 controller 0/0.
Step 2	Router(config-controller)# **mode atm** **Example:**	Specifies that the controller will support ATM encapsulation and create ATM interface 0/0.
Step 3	Router(config-controller)# framing *framing type*	Specifies the T1 framing type as extended super frame or **esf**. When the controller is set to ATM mode, the Controller framing is automatically set to Extended SuperFrame (esf) on T1 and to crc4 on E1.
Step 4	Router(config-controller)# linecode *linecode type*	Specifies the T1 linecode type as **b8zs**. The linecode is automatically set to b8zs on T1 and to hdb3 on E1.

	Command or Action	Purpose
Step 5	Router(config-controller)# **no shutdown**	Ensures that the controller is activated.
Step 6	Router(config-controller)# **exit**	Exits controller configuration mode.
Step 7	Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. For subinterfaces, the default is **multipoint**.
Step 8	Router(config-if)# **pvc***word*] { *vpi*/*vci* | *vci*	Creates an ATM PVC for voice traffic and enters ATM virtual circuit configuration mode. vpi= 0 to 255 vci= 1 to 1023 word= optional PVC identifier (letters only); if you assign a PVC identifier, you can use it to specify this PVC when configuring network dial peers **Note** AAL2 encap is not supported for ilmi and qsaal PVCs.
Step 9	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 10	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak-rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average-rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85 G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 30 byte sample size--max calls x 15 G.729 with 20 byte sample size--max calls x 22 G.729 with 30 byte sample size--max calls x 15 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier.

	Command or Action	Purpose
		You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 11	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specifies the number of seconds between loopback cells, and optionally enables OAM management of the connection. The range for *frequency* is 0 to 600. The default is 10.
Step 12	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled. • The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 13	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 14	Router# **show atm vc**	Verifies the ATM PVC configuration.

Configuring ATM on the Cisco 3660

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC, because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **interface atm <** *slot>/ima<grp#>* [*subinterface-number* [**multipoint** | **point-to-point**]]
2. Router(config-if)# pvc [*name*] *vpi/vci*
3. Router (config-if-atm-vc) # **encapsulation aal2**
4. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
5. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
6. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
7. Router(config-if-atm-vc)# **end**
8. Router# **show atm vc**
9. Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]
10. Router(config-if-atm-vc)# **vcci***pvc-identifier*
11. Router(config-if-atm-vc)# **exit**
12. Router(config-if)# **exit**
13. Router(config)# **dial-peer voice***number***pots**
14. Router(config-dial-peer)# **application MGCPAPP**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm <** *slot>/ima<grp#>* [*subinterface-number* [**multipoint** | **point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. **Note** To configure an IMA group on each ATM interface, enter the IMA group and group number. The default for subinterfaces is **multipoint.** *For all Scenarios* : Set up three subinterfaces for point-to-point.
Step 2	Router(config-if)# pvc [*name*] *vpi/vci*	Creates an ATM PVC for voice traffic and enters ATM virtual circuit configuration mode. **Note** AAL2 encap is not supported for ilmi and qsaal PVCs.
Step 3	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 4	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85

	Command or Action	Purpose
		G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 30 byte sample size--max calls x 15 G.729 with 20 byte sample size--max calls x 22 G.729 with 10 byte sample size--max calls x 43 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst size--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 5	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specify the number of seconds between loopback cells, and optionally enable OAM management of the connection. The range for *frequency* is 0 to 600. The default is 10.
Step 6	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled. • The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 7	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 8	Router# **show atm vc**	Verifies the ATM PVC configuration.
Step 9	Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]	Configures the PVC for the variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM).

	Command or Action	Purpose
		• average rate--Calculate according to the maximum number of calls (max calls) the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: For VoIP: G.711 with 40 or 80 byte sample size: max calls x 128K G.726 with 40 byte sample size: max calls x 85K G.729a with 10 byte sample size: max calls x 85K For VoAAL2: G.711 with 40 byte sample size: max calls x 85K G.726 with 40 byte sample size: max calls x 43K G.729a with 10 byte sample size: max calls x 43K If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by a s much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 10	Router(config-if-atm-vc)# **vcci***pvc-identifier*	Assigns a unique identifier to the PVC.
Step 11	Router(config-if-atm-vc)# **exit**	Exits ATM virtual circuit configuration mode.
Step 12	Router(config-if)# **exit**	Exits interface configuration mode.
Step 13	Router(config)# **dial-peer voice***number***pots**	Enter dial peer configuration mode for the POTS dial peer.
Step 14	Router(config-dial-peer)# **application MGCPAPP**	Initiates the MGCP protocol for the voice ports.

Configuring Voice Band Detection Playout Settings

To configure voice band detection playout buffer delay on Cisco 2600 series and Cisco 3600 series routers , use the following commands beginning in the voice service configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# session protocol aal2
3. Router(config-voice-service-session)# vbd-playout-delay maximum time
4. Router(config-voice-service-session)# vbd-playout-delay minimum time
5. Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}
6. Router(config-voice-service-session)# vbd-playout-delay nominal time
7. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# session protocol aal2 **Example:**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# vbd-playout-delay maximum time	Specifies the maximum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers in milliseconds. The time is set in milliseconds. The range is from 40-1700 milliseconds. The default is set to 200 milliseconds.
Step 4	Router(config-voice-service-session)# vbd-playout-delay minimum time	Specifies the minimum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 4-1700 milliseconds. The default is set to 4 milliseconds.
Step 5	Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}	Configures voice band detection playout delay adaptation mode on a Cisco router. When the vbd-delay-playout mode is set to fixed, jitter buffer is set at a constant delay in milliseconds. When the vbd-delay-playout mode is set to passthrough, jitter buffer is set to DRAIN_FILL for clock compensation. There is no default.
Step 6	Router(config-voice-service-session)# vbd-playout-delay nominal time	Specifies the nominal AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 0-1500 milliseconds. The default is 100 milliseconds.
Step 7	Router(config-voice-service-session)# **end**	Exits voice-service-session configuration mode.

Configuring Subcell Multiplexing for AAL2 Voice

This section describes the configuration tasks necessary to enable AAL2 common part sublayer (CPS) subcell multiplexing when the Cisco 2600 series router or a Cisco 3660 interoperates with a voice interface service module (VISM) in an MGX switch.

To configure the Cisco 2600 series router or the Cisco 3660 to perform subcell multiplexing, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **subcell-mux number**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **subcell-mux number**	Enables subcell multiplexing. The number is time in milliseconds. By default, subcell multiplexing is not enabled.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Verifying the MGCP CAS PBX and AAL2 PVC Configurations

Use these commands to verify the configuration settings:

SUMMARY STEPS

1. Router# **show dial-peer voice sum**
2. Router# **show run**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **show dial-peer voice sum**	Displays the status of the dial peer. The dial peer should be active. If it is not, enter the command: `Router(config-dial-peer)#` **no shut**
Step 2	Router# **show run**	Displays the current configuration settings.

Configuring End-to-End Clocking

The following commands can be used to configure the Cisco 3660 only when there is a TDM switch module on board. For the Cisco 2600 series routers, these commands are automatically allowed.

> **Note** When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC, because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*
2. for Cisco 2600 series:
3. Router(config)**network-clock-select** *priority* **t1** *slot/port*
4. Router(config)**network-clock-select** *priority* **t1** *slot/port*
5. Router(config)**voice-card** *slot*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*	Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the VWIC by entering the keyword **wic** and the slot number 0 on the router.
Step 2	for Cisco 2600 series: **Example:** `Router(config)#` **network-clock-participate** {**nm** | **wic**} *slot*	Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the network module by entering the keyword **nm** and the slot number 1 on the router.

	Command or Action	Purpose

	Example:
	`for Cisco 3660:`
	Example:
	`Router(config)# network-clock-participate nm slot`	

Step 3	Router(config)**network-clock-select** *priority* **t1** *slot/port*	Names a source to provide timing for the network clock and to specify the selection *priority* for this clock source. The priority selection is 1 or 2. Use the **no** form of this command to cancel the selection.
Step 4	Router(config)**network-clock-select** *priority* **t1** *slot/port*	Assigns *priority 1* to ATM interface 0/0 and *priority 2* to controller 1/0.
Step 5	Router(config)**voice-card** *slot*	Enters voice-card configuration mode and sets codec complexity. For *slot* , use a value from 0 to 3 that describes the card location in the module.

Configuring a CAC Master for AAL2 Voice

This section describes the configuration tasks necessary to configure call admission control (CAC) for AAL2 voice. The commands and procedures in this section are common to the Cisco 2600 series and the Cisco 3660 routers.

You can configure a Cisco 2600 series router or a Cisco 3660 as either a CAC master or a CAC slave. By default, this is a CAC slave. You typically configure a CAC master at one end of an ATM trunk and a CAC slave at the opposite end. A Cisco 2600 series router or a Cisco 3660 configured as a master always performs CAC during fax/modem upspeed. A Cisco 2600 series router or a Cisco 3660 configured as a slave sends a request for CAC to the CAC master.

To configure a Cisco 2600 series router or a Cisco 3660 as a CAC master, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC master.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring a CAC Slave for AAL2 Voice

To return a Cisco 2600 series router or a Cisco 3660 to its default operation as a CAC slave, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **no cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **no cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC slave.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring MGCP POTS Dial Peer

To configure MGCP POTS dial peer on the Cisco 2600 series and Cisco 3660, complete the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# dial-peer voice number pots
2. Router(config-dial-peer)# application MGCPAPP
3.
4. Router(config-dial-peer)# exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# dial-peer voice number pots	Enters dial-peer configuration mode for the POTS dial peer.
Step 2	Router(config-dial-peer)# application MGCPAPP	Initiates MGCP for the voice ports.
Step 3	**Example:** `Router(config-dial-peer)# port slot/port:ds0-group`	Associates the dial peer with a specific logical interface. The value of slot is the router location where the voice port adapter is installed. Valid entries are from 0 to 3. The value of port indicates the voice interface card location. Valid entries are 0 or 1. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
Step 4	Router(config-dial-peer)# exit	Exits from the dial-peer configuration mode.

Troubleshooting Tips

- For a good voice quality and to be able to make fax calls, make sure that you configure end-to-end clocking properly, that is, make sure that the T1 controllers particpating in this configuration do not have any errors.
- Make sure that you do not configure bisync tunnelling protocol (BSTUN) and ATM on the Cisco 2650 router simultaneously.

Configuration Tasks for MGCP PRI Backhaul

See the following sections for configuration tasks for MGCP PRI Backhaul for Cisco 2600 series and Cisco 3660 routers:

Configuring MGCP CAS PBX on the Cisco 2600 Series and Cisco 3660

Use the following commands for configuring the Media Gateway Control Protocol (MGCP) CAS PBX on the Cisco 2600 series and the Cisco 3660 routers:

SUMMARY STEPS

1. Router(config)# **mgcp**
2. Router(config)# **mgcp call-agent** *ipaddr* | *hostname*} [*port*] [**service-type** *type*] **version** *version-number*
3. Router(config-if)# **mgcp sgcp restart notify**
4. Router(config-if)# **mgcp modem passthrough [cisco | ca | nse]**
5. Router(config)# **mgcp tse payload***type*
6. Router(config)# **no mgcp timer receive-rtcp**
7. Router(config)# **mgcp timer rtp-nse***timer*
8. Router(config)# **mgcp quarantine mode process**
9. Router(config)# **controller**{**t1** | **e1**} *slot/port*
10. Router(config-controller)# **mode cas**
11. Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type* **tone** *type* **addr info service** *service-type*
12. Router(config-controller)# **exit**
13. Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]
14. Router(config-if-atm-vc)# **vcci***pvc-identifier*
15. Router(config-if-atm-vc)# **exit**
16. Router(config-if)# **exit**
17. Router(config)# **dial-peer voice***number***pots**
18. Router(config-dial-peer)# **application MGCPAPP**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **mgcp**	Starts the MGCP daemon.
Step 2	Router(config)# **mgcp call-agent** *ipaddr* | *hostname*} [*port*] [**service-type** *type*] **version** *version-number*	Configures the MGCP call agent and service type.
Step 3	Router(config-if)# **mgcp sgcp restart notify**	Causes MGCP to send and process SGCP RSIP messages.
Step 4	Router(config-if)# **mgcp modem passthrough [cisco | ca | nse]**	Enables the router to process fax or modem messages. VoAAL2 does not support cisco.
Step 5	Router(config)# **mgcp tse payload***type*	Enables the TSE payload for fax and modem messages.

	Command or Action	Purpose
Step 6	Router(config)# **no mgcp timer receive-rtcp**	Turns off the RTP RTCP transmission interval at the gateway.
Step 7	Router(config)# **mgcp timer rtp-nse***timer*	Turns on the RTP NSE timeout interval at the gateway.
Step 8	Router(config)# **mgcp quarantine mode process**	(Optional) Turns on processing for MGCP quarantine mode.
Step 9	Router(config)# **controller**{**t1** | **e1**} *slot/port*	*For the CAS PBX scenarios only* : Selects the T1/E1 controller 1/0.
Step 10	Router(config-controller)# **mode cas**	*For the CAS PBX scenarios only* : Specifies that the controller will support CAS.
Step 11	Router(config-controller)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type* **tone** *type* **addr info service** *service-type*	*For the CAS PBX scenarios only* : Configures the T1 time slots for CAS calls. The scenarios use the following three digital signal level 0 (DS-0) definitions: • ds0-group 1 time slots 1-8 type e&m-immediate-start • ds0-group 2 time slots 9-16 type e&m-wink-start • ds0-group 3 time slots 17-24 type fxs-ground-start
Step 12	Router(config-controller)# **exit**	*For the CAS PBX scenarios only* : Exits controller configuration mode.
Step 13	Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]	Configures the PVC for the variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average rate--Calculate according to the maximum number of calls (max calls) the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: For VoIP: G.711 with 40 or 80 byte sample size: max calls x 128K G.726 with 40 byte sample size: max calls x 85K G.729a with 10 byte sample size: max calls x 85K For VoAAL2: G.711 with 40 byte sample size: max calls x 85K G.726 with 40 byte sample size: max calls x 43K G.729a with 10 byte sample size: max calls x 43K If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by a s much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less.

	Command or Action	Purpose
		• burst--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 14	Router(config-if-atm-vc)# **vcci***pvc-identifier*	Assigns a unique identifier to the PVC.
Step 15	Router(config-if-atm-vc)# **exit**	Exits ATM virtual circuit configuration mode.
Step 16	Router(config-if)# **exit**	Exits interface configuration mode.
Step 17	Router(config)# **dial-peer voice***number***pots**	Enters dial-peer configuration mode for the POTS dial peer.
Step 18	Router(config-dial-peer)# **application MGCPAPP**	Initiates MGCP for the voice ports. You can enter the MGCPAPP keyword in either uppercase or lowercase.

Configuring ATM on the Cisco 2600 Series

This section describes the ATM configuration tasks necessary to support Voice over ATM using AAL2 on Cisco 2600 series.

Note If any DS0 groups (CAS groups), channel groups, or clear channels are configured on T1/E1 controller 0, you must remove them before configuring VoATM. Because ATM uses all of the DS0 time slots on the controller, the ATM configuration cannot take place if any DS0s on controller 0 are used by other applications.

You must perform the VoATM configuration on the Cisco 2600 series or Cisco 3660 concentrators at both ends of the ATM link.

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

To configure a Cisco 2600 series or Cisco 3660 series concentrator to support VoATM on a T1/E1 trunk, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **controller t1 e1 0/0**
2. Router(config-controller)# **mode atm**
3. Router(config-controller)# framing *framing type*
4. Router(config-controller)# linecode *linecode type*
5. Router(config-controller)# **no shutdown**
6. Router(config-controller)# **exit**
7. Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]
8. Router(config-if)# **pvc***word*] { *vpi*/*vci* | *vci*
9. Router (config-if-atm-vc) # **encapsulation aal2**
10. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
11. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
12. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
13. Router(config-if-atm-vc)# **end**
14. Router# **show atm vc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller t1 e1 0/0**	Selects the T1 or E1 controller 0/0.
Step 2	Router(config-controller)# **mode atm** **Example:**	Specifies that the controller will support ATM encapsulation and create ATM interface 0/0.
Step 3	Router(config-controller)# framing *framing type*	Specifies the T1 framing type as Extended SuperFrame (**esf)**. When the controller is set to ATM mode, the Controller framing is automatically set to Extended SuperFrame (esf) on T1 and to crc4 on E1.
Step 4	Router(config-controller)# linecode *linecode type*	Specifies the T1 linecode type as **b8zs**. The linecode is automatically set to b8zs on T1 and to hdb3 on E1.
Step 5	Router(config-controller)# **no shutdown**	Ensures that the controller is activated.
Step 6	Router(config-controller)# **exit**	Exits controller configuration mode.
Step 7	Router(config)# **interface atm** *slot/port subinterface-number* **multipoint** |**point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. For subinterfaces, the default is **multipoint**.
Step 8	Router(config-if)# **pvc***word*] { *vpi*/*vci* | *vci*	Creates an ATM PVC for voice traffic and enters ATM virtual circuit configuration mode.

	Command or Action	Purpose
		vpi= 0 to 255 vci= 1 to 1023 word= optional PVC identifier (letters only); if you assign a PVC identifier, you can use it to specify this PVC when configuring network dial peers **Note** AAL2 encap is not supported for ilmi and qsaal PVCs.
Step 9	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 10	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak-rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average-rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85 G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 30 byte sample size--max calls x 15 G.729 with 20 byte sample size--max calls x 22 G.729 with 30 byte sample size--max calls x 15 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 11	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specifies the number of seconds between loopback cells, and optionally enables OAM management of the connection. The range for *frequency* is 0 to 600. The default is 10.

	Command or Action	Purpose
Step 12	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled. • The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 13	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 14	Router# **show atm vc**	Verifies the ATM PVC configuration.

Configuring ATM on the Cisco 3660

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC, because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **interface atm** *slot/ima grp#* [*subinterface-number* [**multipoint** | **point-to-point**]]
2. Router(config-if)# pvc [*name*] *vpi/vci*
3. Router (config-if-atm-vc) # **encapsulation aal2**
4. Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*
5. Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*
6. Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*
7. Router(config-if-atm-vc)# **end**
8. Router# **show atm vc**
9. Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]
10. Router(config-if-atm-vc)# **vcci***pvc-identifier*
11. Router(config-if-atm-vc)# **exit**
12. Router(config-if)# **exit**
13. Router(config)# **dial-peer voice***number***pots**
14. Router(config-dial-peer)# **application MGCPAPP**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot/ima grp#* [*subinterface-number* [**multipoint** | **point-to-point**]]	Enters interface configuration mode to configure ATM interface 0/0 or an ATM subinterface. **Note** To configure an IMA group on each ATM interface, enter the IMA group and group number. The default for subinterfaces is **multipoint.** *For all Scenarios* : Set up three subinterfaces for point-to-point.
Step 2	Router(config-if)# pvc [*name*] *vpi/vci*	Creates an ATM PVC for voice traffic and enters ATM virtual circuit configuration mode. **Note** AAL2 encap is not supported for ilmi and qsaal PVCs.
Step 3	Router (config-if-atm-vc) # **encapsulation aal2**	Sets the encapsulation of the PVC to support AAL2 voice traffic. This automatically creates channel identifiers (CIDs) 1 through 255.
Step 4	Router(config-if-atm-vc)# **vbr-rt***peak-rate average-rate* [*burst*	Configures the PVC for variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM). • average rate--Calculate according to the maximum number of calls the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: G.711 with 40 or 80 byte sample size--max calls x 85

	Command or Action	Purpose
		G.726 with 40 or 80 byte sample size--max calls x 43 G.729 with 30 byte sample size--max calls x 15 G.729 with 20 byte sample size--max calls x 22 G.729 with 10 byte sample size--max calls x 43 If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by as much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst size--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 5	Router(config-if-atm-vc)# **oam-pvc manage**] [*frequency*	(Optional) Configures transmission of end-to-end F5 OAM loopback cells on a PVC, optionally specify the number of seconds between loopback cells, and optionally enable OAM management of the connection. The range for *frequency* is 0 to 600. The default is 10.
Step 6	Router(config-if-atm-vc)# **oam retry***up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is supported only if OAM management is enabled. • The value of *up-count* is the number of OAM loopback cell responses received to change the PVC connection to up. The range is 1 to 600; the default is 3. • The value of *down-count* is the number of OAM loopback cell responses not received to change the PVC connection to down. The range is 1 to 600; the default is 5. • The value of *retry-frequency* is the number of seconds between loopback cells sent to verify the down state of a PVC. The range is 1 to 1000; the default is 1. **Note** Enter the **oam retry** command only once with all the arguments in the order shown. The first number always specifies *up-count* ; the second *down-count* , and the third *retry-frequency* .
Step 7	Router(config-if-atm-vc)# **end**	Exits configuration mode.
Step 8	Router# **show atm vc**	Verifies the ATM PVC configuration.
Step 9	Router(config-if-atm-vc)# **vbr-rt***peak-rateaverage-rate* [*burst*]	Configures the PVC for the variable-bit-rate real-time (voice) traffic. Guidelines for setting the peak rate, average rate, and burst size are as follows: • peak rate--If it does not exceed your carrier's allowable rate, set to the line rate (for example, 1536 kbps for T1-ATM).

	Command or Action	Purpose
		• average rate--Calculate according to the maximum number of calls (max calls) the PVC will carry times the bandwidth per call. The following formulas give you the average rate in kbps: for VoIP: G.711 with 40 or 80 byte sample size: max calls x 128K G.726 with 40 byte sample size: max calls x 85K G.729a with 10 byte sample size: max calls x 85K for VoAAL2: G.711 with 40 byte sample size: max calls x 85K G.726 with 40 byte sample size: max calls x 43K G.729a with 10 byte sample size: max calls x 43K If voice activity detection (VAD) is enabled, the bandwidth usage is reduced by a s much as 12 percent with the maximum number of calls in progress. With fewer calls in progress, bandwidth savings are less. • burst--Set the burst size as large as possible, and never less than the minimum burst size. Guidelines are as follows: The minimum burst size is 4 x the number of voice calls. The maximum burst size is the maximum allowed by the carrier. You can calculate the value using the calculator at the following URL: http://www-vnt/SPUniv/DSP/Codec_Calc1.asp
Step 10	Router(config-if-atm-vc)# **vcci***pvc-identifier*	Assigns a unique identifier to the PVC.
Step 11	Router(config-if-atm-vc)# **exit**	Exits ATM virtual circuit configuration mode.
Step 12	Router(config-if)# **exit**	Exits interface configuration mode.
Step 13	Router(config)# **dial-peer voice***number***pots**	Enter dial peer configuration mode for the POTS dial peer.
Step 14	Router(config-dial-peer)# **application MGCPAPP**	Initiates the MGCP protocol for the voice ports.

Configuring Voice Band Detection Playout Settings

To configure voice band detection playout buffer delay on Cisco 2600 series and Cisco 3600 series routers , use the following commands beginning in the voice service configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# session protocol aal2
3. Router(config-voice-service-session)# vbd-playout-delay maximum time
4. Router(config-voice-service-session)# vbd-playout-delay minimum time
5. Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}
6. Router(config-voice-service-session)# vbd-playout-delay nominal time
7. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# session protocol aal2 **Example:**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# vbd-playout-delay maximum time	Specifies the maximum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers in milliseconds. The time is set in milliseconds. The range is from 40-1700 milliseconds. The default is set to 200 milliseconds.
Step 4	Router(config-voice-service-session)# vbd-playout-delay minimum time	Specifies the minimum AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 4-1700 milliseconds. The default is set to 4 milliseconds.
Step 5	Router(config-voice-service-session)# vbd-playout-delay mode {fixed | passthrough}	Configures voice band detection playout delay adaptation mode on a Cisco router. When the vbd-delay-playout mode is set to fixed, jitter buffer is set at a constant delay in milliseconds. When the vbd-delay-playout mode is set to passthrough, jitter buffer is set to DRAIN_FILL for clock compensation. There is no default.
Step 6	Router(config-voice-service-session)# vbd-playout-delay nominal time	Specifies the nominal AAL2 voice band detection playout delay buffer on Cisco 2600 series and Cisco 3660 routers. The time is set in milliseconds. The range is from 0-1500 milliseconds. The default is 100 milliseconds.
Step 7	Router(config-voice-service-session)# **end**	Exits voice-service-session configuration mode.

Configuring Subcell Multiplexing for AAL2 Voice

This section describes the configuration tasks necessary to enable AAL2 common part sublayer (CPS) subcell multiplexing when the Cisco 2600 series router or a Cisco 3660 interoperates with a voice interface service module (VISM) in an MGX switch.

To configure the Cisco 2600 series router or the Cisco 3660 to perform subcell multiplexing, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **subcell-mux number**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **subcell-mux number**	Enables subcell multiplexing. The number is time in milliseconds. By default, subcell multiplexing is not enabled.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Verifying the MGCP CAS PBX and AAL2 PVC Configurations

Use these commands to verify the configuration settings:

SUMMARY STEPS

1. Router# **show dial-peer voice sum**
2. Router# **show run**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **show dial-peer voice sum**	Displays the status of the dial peer. The dial peer should be active. If it is not, enter the command: `Router(config-dial-peer)#` **no shut**
Step 2	Router# **show run**	Displays the current configuration settings.

Configuring End-to-End Clocking

The following commands can be used to configure the Cisco 3660 only when there is a TDM switch module on board. For the Cisco 2600 series these commands are automatically allowed.

Note When verifying your ATM PVC connectivity, note that you cannot enter the **ping** command over a voice PVC because the command applies to data only. If you have data and voice PVCs set to the same destination, you can enter the **ping** command over the data PVC.

SUMMARY STEPS

1. Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*
2. for Cisco 2600 series:
3. Router(config)**network-clock-select** *priority* **t1** *slot/port*
4. Router(config)**network-clock-select** *priority* **t1** *slot/port*
5. Router(config)**voice-card** *slot*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **network-clock-participate**{**nm** | **wic**} *slot*	Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the VWIC by entering the keyword **wic** and the slot number 0 on the router.
Step 2	for Cisco 2600 series: **Example:** `Router(config)#` **network-clock-participate** {**nm** | **wic**} *slot*	Enables the Cisco 2600 series router or the Cisco 3660 to receive clock signals from the network module by entering the keyword **nm** and the slot number 1 on the router.

	Command or Action	Purpose

	Example:
	`for Cisco 3660:`
	Example:
	`Router(config)# network-clock-participate {nm} slot`	

Step 3	Router(config)**network-clock-select** *priority* **t1** *slot/port*	Names a source to provide timing for the network clock and to specify the selection *priority* for this clock source. The priority selection is *1* or *2* . Use the **no** form of this command to cancel the selection.
Step 4	Router(config)**network-clock-select** *priority* **t1** *slot/port*	Assigns *priority 1* to ATM interface 0/0 and *priority 2* to controller 1/0.
Step 5	Router(config)**voice-card** *slot*	Enters voice-card configuration mode and set codec complexity. For *slot,* use a value from 0 to 3 that describes the card location in the module.

Configuring a CAC Master for AAL2 Voice

This section describes the configuration tasks necessary to configure call admission control (CAC) for AAL2 voice. The commands and procedures in this section are common to the Cisco 2600 series and Cisco 3660.

You can configure a Cisco 2600 series router or a Cisco 3660 as either a CAC master or a CAC slave. By default, this is a CAC slave. You typically configure a CAC master at one end of an ATM trunk and a CAC slave at the opposite end. A Cisco 2600 series router or a Cisco 3660 configured as a master always performs CAC during fax/modem upspeed. A Cisco 2600 series router or a Cisco 3660 configured as a slave sends a request for CAC to the CAC master.

To configure a Cisco 2600 series router or a Cisco 3660 as a CAC master, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC master.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring a CAC Slave for AAL2 Voice

To return a Cisco 2600 series router or a Cisco 3660 to its default operation as a CAC slave, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **voice service voatm**
2. Router(config-voice-service)# **session protocol aal2**
3. Router(config-voice-service-session)# **no cac master**
4. Router(config-voice-service-session)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **voice service voatm**	Enters voice-service configuration mode.
Step 2	Router(config-voice-service)# **session protocol aal2**	Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	Router(config-voice-service-session)# **no cac master**	Configures this Cisco 2600 series router or a Cisco 3660 as a CAC slave.
Step 4	Router(config-voice-service-session)# **end**	Exits configuration mode.

Configuring Backhaul Session Manager

The backhaul session manager operates on the media gateway and enables signaling applications to backhaul signaling information to a remote or local virtual switch controller (VSC), and also provides redundancy and transparent management of transport paths.

To configure the backhaul session manager, log on to the media gateway and complete the following tasks as required for your application:

Creating Session Sets and Groups and Sessions

To create session sets, session groups, and sessions on the Cisco media gateway, complete the following steps starting in global configuration mode:

SUMMARY STEPS

1. Router(config)# **backhaul-session-manager**
2. Router(config-bsm)# **set** *set-name* **client ft nft**
3. Router(config-bsm)# **group** *group-name* **set** *set-name*
4. Router(config-bsm)# **session group***group-name remote_ip remote_port local_ip local_port priorit* y

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **backhaul-session-manager**	Enters backhaul session manager configuration mode.

Step 2	Router(config-bsm)# **set** *set-name* **client ft nft**	Creates a session set and specifies its parameters:
		• *set-name* --A word you select to identify the session-set
		• **client** --Required for PRI backhaul; specifies that the session set function as a client
		• Fault-tolerance option:
		  • **ft** = fault-tolerant
		  • **nft** = non-fault-tolerant
		Note For fault-tolerant operation, you must configure more than one group in this session set. If only one group will be configured in this session-set, you must specify **nft**.
		Note If you configure the session set for non-fault-tolerant operation, you should also configure the Cisco VSC3000 for non-fault-tolerant operation. See the Configuring the Cisco VSC3000, on page 306.

Step 3	Router(config-bsm)# **group** *group-name* **set** *set-name*	Adds a new session group to a specified session set. • *group-name* --A word you select to identify the new session group • *set-name* --The session-set to which you are adding the new session group

	Command or Action	Purpose
		Repeat this step to add additional session groups to a session set.
Step 4	Router(config-bsm)# **session group***group-name remote_ip remote_port local_ip local_port priorit* y	Adds a session to a session group and specifies the interfaces and selection priority for the session. • *group-name* --The session group to which you are adding this session. • *remote_ip* --IP address of the Cisco VSC3000 server at the remote end of this backhaul link. • *remote_port* --The UDP port number on the Cisco VSC3000 server at the remote end of this backhaul link; the range is 1024 to 9999. Make sure that this number is not already being used by another service on the Cisco VSC3000, such as MGCP. • *local_ip* --The IP address of the media gateway port used for signaling backhaul. • *local_port* --The UDP port number of the media gateway port used for signaling backhaul; the range is 1024 to 9999 • *priority* --The priority within the session group. The range is 0 to 9999; 0 is the highest priority. **Note** Although the Cisco IOS software allows you to configure multiple sessions with the same priority in a session group, Cisco Systems recommends that the priority of each session be unique within a session group. Repeat this step to create additional sessions in a session group.

Changing Default Values of Session-Group Parameters

If you need to change the default values of session-group parameters, complete the following commands as required, in backhaul-session-manager configuration mode:

Caution Do not change the session-group parameters unless instructed to do so by Cisco technical support. Sessions might fail if the relationships among parameters are not set correctly.

Command	Purpose
`Router(config-bsm)#` **group** *group-name* **auto-reset** *number-of-auto-resets*	Specifies the maximum number of auto resets before the connection is considered failed. The range is 0 to 255. The default is 5.
`Router(config-bsm)#` **group** *group-name* **cumulative-ack** *number-of-segments*	Specifies the maximum number of (RUDP) segments that will be received before sending an acknowledgement. The range is 0 to 255. The default is 3.
`Router(config-bsm)#` **group** *group-name* **out-of-sequence** *number-of-segments*	Specifies the maximum number of out-of-sequence segments that will be received before an acknowledgement is sent. The range is 0 to 255. The default is 3.
`Router(config-bsm)#` **group** *group-name* **receive** *window-size*	Specifies the maximum window size for the receiver. The range is 1 to 65. The default is 32.
`Router(config-bsm)#` **group** *group-name* **retrans** *resend-attempts*	Specifies the maximum number of times reliable user data protocol (RUDP) attempts to resend a segment before declaring the connection broken. The range is 0 to 255. The default is 2.
`Router(config-bsm)#` **group** *group-name* **timer cumulative-ack** *milliseconds*	Specifies the maximum number of milliseconds RUDP delays before sending an acknowledgement for a received segment. The range is 100 to 65535 . The default is 300.
`Router(config-bsm)#` **group** *group-name* **timer keepalive** *milliseconds*	Specifies the number of milliseconds RUDP waits before sending a keepalive segment. The range is 0 to 65535. The default is 200.
`Router(config-bsm)#` **group** *group-name* **timer retransmit** *milliseconds*	Specifies the number of milliseconds RUDP waits to receive an acknowledgement for a segment. The range is 100 to 65535. The default is 600.
`Router(config-bsm)#` **group** *group-name* **timer transfer-state** *milliseconds* `Router(config-bsm)#` **exit**	Specifies the number of milliseconds RUDP waits to receive a selection of a new session from the application during a transfer state. The range is 0 to 65535. The default is 600.

Configuring ISDN Signaling Backhaul

To configure the ISDN Q.931 signaling backhaul parameters, log on to the media gateway and complete the following steps starting in global configuration mode. Repeat this procedure for each T1 interface on the media gateway that will use backhaul.

SUMMARY STEPS

1. Router(config)# **controller**{**t1** | **e1**}*controller-number*
2. Router(config-control)# **pri-group timeslots 1-24 service mgcp**
3. Router(config-control)# **exit**
4. Router(config)# **interface serial***controller-number***:23**
5. Router(config-if)# **isdn switch-type***switch-type*
6. Router(config-if)# **isdn bind-L3 backhaul** *set-name*
7. Router(config-if)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **controller**{**t1** | **e1**}*controller-number*	Enters controller configuration mode and specifies a controller for the PRI interface. Controller numbers are: **0/0**, **0/1**, **1/0**, **1/1**, **2/0**, **2/1**, **3/0**, **3/1**, **4/0**, **4/1**, **5/0**, **5/1**
Step 2	Router(config-control)# **pri-group timeslots 1-24 service mgcp**	Creates a serial D-channel interface for signaling backhaul and specifies control protocol MGCP for signaling backhaul. • The controller time slots cannot be shared between backhaul and other Layer 3 protocols.
Step 3	Router(config-control)# **exit**	Exits from controller configuration mode.
Step 4	Router(config)# **interface serial***controller-number***:23**	Enters interface configuration mode for the D-channel signaling backhaul interface. Enter a controller number that matches the controller number specified in Step 1.
Step 5	Router(config-if)# **isdn switch-type***switch-type*	Configures the D-channel interface to match the ISDN switch type. Examples of ISDN switch types include **primary-4ess, primary-5ess, primary-nec5.** • This can be done in either global or interface configuration mode.
Step 6	Router(config-if)# **isdn bind-L3 backhaul** *set-name*	Configures ISDN to backhaul Q.931 to the Cisco VSC3000. • You must use the set name of a session set that was defined in Step 2 of the Creating Session Sets and Groups and Sessions, on page 301. • In the example, "L" is shown for clarity. You can enter lower-case "l".

	Command or Action	Purpose
Step 7	Router(config-if)# **exit**	Exits the interface configuration mode.

Configuring Fast Ethernet for Signaling Backhaul Compatibility

If your media gateway has 10/100 BASE-T Fast Ethernet capability, configure the Fast Ethernet interface not to use auto negotiation.

Caution When the Fast Ethernet interface is configured for auto-negotiation, it can take up to 2 seconds for this interface to be enabled when the interface has to initialize. Two examples where the interface initializes are execution of the **no shut** command and disconnection or reconnection of the Ethernet cable. Auto-negotiation affects the traffic flow on the Ethernet interface and can, therefore, interrupt the traffic flow on existing RUDP connections, causing them to fail. To avoid these problems, the Fast Ethernet interface should not be configured for auto-negotiation. Instead, set the duplex and speed parameters according to the requirements of the network.

To reconfigure the Fast Ethernet interface for specified duplex and speed operation, complete the following steps beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **int***Ethernet-port-number*
2. Router(config-if)# **duplex full half**
3. Router(config-if)# **speed 10 100**}
4. Router(config-if)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **int***Ethernet-port-number*	Enters Ethernet interface configuration mode for the specified Ethernet port.
Step 2	Router(config-if)# **duplex full half**	Configures the Ethernet port for full-duplex or half-duplex operation.
Step 3	Router(config-if)# **speed 10 100**}	Configures the Ethernet port to operate at 10 Mbps or 100 Mbps.
Step 4	Router(config-if)# **exit**	Exits from interface configuration mode.

Configuring the Cisco VSC3000

The Cisco VSC3000 is the signaling controller software that provides call control and runs on a UNIX server such as a Sun Netra 1800. Man Machine Language (MML) is the user interface into the signaling controller software. You use this interface to configure parameters of your signaling controller software and to display information about the current settings.

Note If the Cisco VSC3000 is set up for fault-tolerant operation, configure the backhaul session manager also for fault-tolerant operation. For more information, refer to the *Cisco MGC Software Release 7 Provisioning Guide* .

To configure the Cisco VSC3000 to perform signaling backhaul, log on to the UNIX server and complete the MGCP service provisioning procedure as follows:

SUMMARY STEPS

1. mml> **prov-add:extnode:name=** *media-gateway-name* ,
2. **desc=** *media-gateway-name*
3. mml> **prov-add:ipfaspath:name=** *ipfaspath-name* ,
4. **extnode=** *media-gateway-name* ,
5. **mdo=** *ISDN-varient* ,
6. **custgrpid=** *customer-group-ID* ,
7. **side=** *equipment-location* ,
8. **desc=** *description*
9. mml> **prov-add:iplnk:name=** *iplink-name* ,
10. **if=enif** *interface-number* ,
11. **ipaddr=IP_Addr** *number* ,
12. **port=** *port-number* ,
13. **pri=** *priority-number* ,
14. **peeraddr=** *IP-address* ,
15. **peerport=** *port-number* ,
16. **sigslot=** *slot-number* ,
17. **sigport=** *port-number* ,
18. **svc=** *ipfaspath-name* ,
19. **desc=** *description*
20. mml>**prov-add:mgcppath:name=** *MGCP-path-name* ,
21. **extnode=** *ipfaspath-name* ,
22. **desc=** *description*
23. mml>**prov-add:iplnk:name=** *clink6* ,
24. **if=** *enif1* ,
25. **ipaddr=IP_Addr** *number* ,
26. **port=2427,**
27. **peeraddr=** *IP-address* ,
28. **peerport=2427,**
29. **svc=** *mgcp-service-name* ,
30. **pri=1,**
31. **desc=** *description*

DETAILED STEPS

	Command or Action	Purpose
Step 1	mml> **prov-add:extnode:name=** *media-gateway-name* ,	Assigns a name to the media gateway (the external node) at the far end of a backhaul link.

	Command or Action	Purpose
Step 2	**desc=** *media-gateway-name*	Provides a description of the media gateway (MG).
Step 3	mml> **prov-add:ipfaspath:name=** *ipfaspath-name* **,**	Adds an IP path for D-channel transport (ipfaspath) from the Cisco VSC3000 to a media gateway and assigns it a path name.
Step 4	**extnode=** *media-gateway-name* **,**	Specifies the media gateway (external node) at the opposite end of the IP path; the name must match the media gateway name assigned in Step 1.
Step 5	**mdo=** *ISDN-varient* **,**	Specifies the ISDN variant. Options include: • **ETSI_300_102** • **ETSIS_300_102_C1** • **ATT_41459** • **ATT_41459_C2** • **BELL_1268** • **ETSI_300_172** • **BELL_1268_C3**
Step 6	**custgrpid=** *customer-group-ID* **,**	Assigns a customer group ID (the dial plan to use for this connection).
Step 7	**side=** *equipment-location* **,**	Defines the Cisco VSC3000 as network side or user side. The Cisco VSC3000 is normally network side, opposite to the PBX, which is normally the user side. Enter **network,** or **user,**.
Step 8	**desc=** *description*	Describes the function of this IP path (backhaul service to a specified media gateway, for example Backhaul service to 3660-6).
Step 9	mml> **prov-add:iplnk:name=** *iplink-name* **,**	Adds an IP link for the PRI D-channel and assigns it a name.
Step 10	**if=enif** *interface-number* **,**	The Ethernet interface name for the Cisco VSC3000 Ethernet card (typically enif1).
Step 11	**ipaddr=IP_Addr** *number* **,**	The IP address of the Cisco VSC3000 Ethernet port as defined in ../etc/XECfgParm.dat (for example, IP_Addr1).
Step 12	**port=** *port-number* **,**	The port number on the Cisco VSC3000.
Step 13	**pri=** *priority-number* **,**	The selection priority of this IP link. (1, 2 and so on; this should match the selection priority specified on the media gateway for this IP link.)
Step 14	**peeraddr=** *IP-address* **,**	The IP address of the media gateway.
Step 15	**peerport=** *port-number* **,**	The port number on the media gateway; does not have to match the Cisco VSC3000 port
Step 16	**sigslot=** *slot-number* **,**	The physical card slot in the media gateway.

	Command or Action	Purpose
Step 17	**sigport=** *port-number* ,	The PRI port number in the media gateway (= the T1/E1 controller number).
Step 18	**svc=** *ipfaspath-name* ,	The IP path that this IP link is assigned to, which matches the *ipfaspath-name* assigned in Step 2.
Step 19	**desc=** *description*	Optional description of this IP link. For example, **IP link-backhaul svc 3660-6**could describe an IP link for backhaul service to media gateway 3660-6.
Step 20	mml>**prov-add:mgcppath:name=** *MGCP-path-name* ,	Defines an MGCP control path. For example, mgcp36606 could define an MGCP path to media gateway 3660-6.
Step 21	**extnode=** *ipfaspath-name* ,	Associates the MGCP control path with an IP path for D-channel transport. The *ipfaspath-name* must match the ipfaspath-name specified inStep 2.
Step 22	**desc=** *description*	Optional description of this MGCP control path. For example, MGCP service to 3660-6 could describe the function of this MGCP control path.
Step 23	mml>**prov-add:iplnk:name=** *clink6* ,	Adds an IP link for the MGCP control path.
Step 24	**if=** *enif1* ,	The Ethernet interface name for the Cisco VSC3000 Ethernet card (typically enifl).
Step 25	**ipaddr=IP_Addr** *number* ,	The IP address of the Cisco VSC3000 Ethernet port as defined in ../etc/XECfgParm.dat (for example, IP_Addr1).
Step 26	**port=2427,**	The port used by the IP link for the MGCP control path on the Cisco VSC3000 (2427 is pre-defined for MGCP use).
Step 27	**peeraddr=** *IP-address* ,	The IP address of the media gateway connected to this IP link.
Step 28	**peerport=2427,**	The IP port at the media gateway for this IP link (2427 is pre-defined for MGCP use).
Step 29	**svc=** *mgcp-service-name* ,	A name of the MGCP signaling service supported by this IP link. For example, mgcp36606 could be the name for MGCP signaling service to 3660-6).
Step 30	**pri=1,**	Selection priority for this IP link(1, 2, and so on).
Step 31	**desc=** *description*	Optional description of the IP link for the MGCP control path. For example, MGCP link to 3660-6 could describe the IP link for the MGCP path to 3660-6.

Verifying the Configuration

SUMMARY STEPS

1. Enter the **show isdn status**command to verify successful ISDN configuration for backhaul. The following output shows that Layers 1, 2, 3 are enabled and active. Layer 3 shows the number of active ISDN calls.
2. Enter the **show backhaul-session-manager set all** command to display all session sets. This set contains one group called grp1, and it is configured in fault-tolerant mode.
3. Enter the **show backhaul-session-manager group status all** command to display the status of all session-groups.
4. Enter the **show backhaul-session-manager session all** command to display all sessions.

DETAILED STEPS

Step 1 Enter the **show isdn status**command to verify successful ISDN configuration for backhaul. The following output shows that Layers 1, 2, 3 are enabled and active. Layer 3 shows the number of active ISDN calls.
In the example below, notice that the Layer 2 protocol is Q.921, and the Layer 3 protocol is BACKHAUL. This verifies that it is configured to backhaul ISDN. Also, if you are connected to a live line, you should see that Layer 1 status is ACTIVE and that layer 2 state is MULTIPLE_FRAME_ESTABLISHED. This means that the ISDN line is up and active.

Example:

```
Router# show isdn status
*00:03:34.423 UTC Sat Jan 1 2000
Global ISDN Switchtype = primary-net5
ISDN Serial1:23 interface
        dsl 0, interface ISDN Switchtype = primary-net5
        L2 Protocol = Q.921  L3 Protocol(s) = BACKHAUL
    Layer 1 Status:        ACTIVE    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        NLCB:callid=0x0, callref=0x0, state=31, ces=0 event=0x0
        NLCB:callid=0x0, callref=0x0, state=0, ces=1 event=0x0
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Number of active calls = 0
    Number of available B-channels = 23
    Total Allocated ISDN CCBs = 0
Router#
```

Step 2 Enter the **show backhaul-session-manager set all** command to display all session sets. This set contains one group called grp1, and it is configured in fault-tolerant mode.

Example:

```
Router# show backhaul-session-manager set all
Session-Set
   Name   :set1
   State  :BSM_SET_OOS

   Mode   :Fault-Tolerant(FT)
   Option :Option-Client
   Groups :1
   statistics
        Successful switchovers:0
        Switchover Failures:0
```

```
        Set Down Count 0
        Group:grp1
```

Possible states are:

SESS_SET_IDLE--A session set has been created.

SESS_SET_OOS--A session has been added to session group. No ACTIVE notification has been received from the Cisco VSC3000.

SESS_SET_ACTIVE_IS--An ACTIVE notification has been received over one in-service session group. STANDBY notification has not been received on any available session group(s).

SESS_SET_STNDBY_IS--A STANDBY notification is received, but no in-service active session group available.

SESS_SET_FULL_IS--A session group in-service that has ACTIVE notification, and at least one session group in-service has STANDBY notification.

SESS_SET_SWITCH_OVER--An ACTIVE notification is received on session group in-service, that had received STANDBY notification.

Step 3 Enter the **show backhaul-session-manager group status all** command to display the status of all session-groups. The status is either Group-OutOfService (no session in the group has been established) or Group-Inservice (at least one session in the group has been established).

The Status (use) is either Group-Standby (the Cisco VSC3000 connected to the other end of this group will go into standby mode), Group-Active (the Cisco VSC3000 connected to the other end of this group will be the active Cisco VSC3000), or Group-None (the Cisco VSC3000 has not declared its intent yet).

Example:

```
Router# show backhaul-session-manager group status all
Session-Group
Group Name   :grp1
   Set Name     :set1
   Status       :Group-OutOfService
   Status (use) :Group-None
```

Step 4 Enter the **show backhaul-session-manager session all** command to display all sessions.
The State is OPEN (the connection is established), OPEN_WAIT (the connection is awaiting establishment), OPEN_XFER (session failover is in progress for this session, which is a transient state), or CLOSE (this session is down, also a transient state). The session moves to OPEN_WAIT after waiting a fixed amount of time.

The Use-status field indicates whether PRI signaling traffic is being transported over this session. The field will be either OOS (this session is not being used to transport signaling traffic) or IS (this session is being used currently to transport all PRI signaling traffic). The User-status field indicates the connection status.

Example:

```
Router# show backhaul-session-manager session all

Session information --
Session-id:35
  Group:grp1
Configuration:
     Local:10.1.2.15      , port:8303
    Remote:10.5.0.3       , port:8303
  Priority:2
  RUDP Option:Client, Conn Id:0x2
State:
  Status:OPEN_WAIT, Use-status:OOS
```

```
Statistics:
  # of resets:0
  # of auto_resets 0
  # of unexpected RUDP transitions (total) 0
  # of unexpected RUDP transitions (since last reset) 0
  Receive pkts -  Total:0 , Since Last Reset:0
  Recieve failures -  Total:0 ,Since Last Reset:0
  Transmit pkts - Total:0, Since Last Reset:0
```

Example:

```
  Transmit Failures (PDU Only)
         Due to Blocking (Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  Transmit Failures (NON-PDU Only)
         Due to Blocking(Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  RUDP statistics
         Open failures:0
         Not ready failures:0
         Conn Not Open failures:0
         Send window full  failures:0
         Resource unavailble failures:0
         Enqueue failures:0
```

Configuring MGCP POTS Dial Peer

To configure MGCP POTS dial peer on the Cisco 2600 series and Cisco 3660, complete the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# dial-peer voice number pots
2. Router(config-dial-peer)# application MGCPAPP
3. *Router(config-dial-peer)# port slot/port:ds0-group*
4. Router(config-dial-peer)# exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# dial-peer voice number pots	Enters the dial-peer configuration mode for the POTS dial peer.
Step 2	Router(config-dial-peer)# application MGCPAPP	Initiates MGCP for the voice ports.
Step 3	*Router(config-dial-peer)# port slot/port:ds0-group*	*Associates the dial peer with a specific logical interface.* *The value of slot is the router location where the voice port adapter is installed. Valid entries are from 0 to 3.*

	Command or Action	Purpose
	Example:	*The value of port indicates the voice interface card location. Valid entries are 0 or 1.* *Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.*
Step 4	Router(config-dial-peer)# exit	Exits dial-peer configuration mode.

Monitoring and Maintaining

Monitoring MGCP CAS PBX and AAL2 PVC Configurations

Use these commands at any time to monitor the MGCP configuration:

Command	Purpose
`Router#` **`show mgcp connection	endpoint	statistics`**	Displays all active MGCP connections on the router.
`Router#` **debug mgcp** [**all** | **errors** | **events** | **packets** | **parser**]	Turns on debugging for the gateway.
`Router#` **clear mgcp statistics**	Resets the MGCP statistical counters.

Monitoring and Maintaining Signaling Backhaul

Use the following commands as required to monitor and maintain the signaling backhaul sessions and the connection to the Cisco VSC3000:

Command	Purpose
Router# **clear backhaul-session-manager group**	Resets the statistics for all available session groups or a specified session group.
Router# **show backhaul-session-manager set**	Displays status, statistics, or configuration of all available session sets.
Router# **show backhaul-session-manager group**	Displays status, statistics, or configuration of all available session groups.
Router# **show backhaul-session-manager session**	Displays status, statistics, or configuration of all available sessions.
Router# **show isdn status**	Displays status of ISDN backhaul. If the connection to the Cisco VSC3000 is lost, the router shuts down Layer 2 so that it cannot receive more calls. When the Cisco VSC3000 connection is back up, you may use this to verify that Layer 2 was also brought back up correctly.

Configuration Examples

Cisco 2600 Series

MGCP CAS Voice FAX Call Examples

Originating Gateway Configuration Example

```
2650-org# show run
Building configuration...
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2650-org
!
enable password lab
!
```

```
!
!
memory-size iomem 10
voice-card 1
no ip subnet-zero
no ip domain-lookup
ip dhcp smart-relay
!
mgcp
mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
mgcp modem passthrough voaal2 mode nse
mgcp sdp simple
mgcp default-package dt-package
no mgcp timer receive-rtcp
!
!
controller T1 0/0
 mode atm
 framing esf
 clock source internal
 linecode b8zs
!
controller T1 0/1
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
 ds0-group 2 timeslots 2 type e&m-immediate-start
!
controller T1 1/1
!
interface Ethernet0/0
 ip address 1.9.46.170 255.255.0.0
 no cdp enable
!
interface Ethernet0/1
 no ip address
 shutdown
 no cdp enable
!
interface ATM0/0
 no ip address
 ip mroute-cache
 atm idle-cell-format itu
 atm uni-version 4.0
 atm voice aal2 aggregate-svc bandwidth 1500
 atm voice aal2 aggregate-svc traffic-parameters 1500 1500 65000
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa 111111111111.01 application aal2xgcp
 atm ilmi-keepalive
 pvc 0/5 qsaal
 !
 pvc 0/16 ilmi
 !
!
ip default-gateway 1.9.0.1
ip kerberos source-interface any
ip classless
no ip http server
!
no cdp run
!
snmp-server engineID local 00000009020000505474 7B80
no snmp-server ifindex persist
snmp-server forwarder
snmp-server manager
!
voice-port 1/0:1
!
voice-port 1/0:2
!
dial-peer cor custom
```

```
!
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 1/0:1
 forward-digits all
!
dial-peer voice 2 pots
 application mgcpapp
 port 1/0:2
 forward-digits all
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password lab
 login
!
end
2650-org#
```

Terminating Gateway Configuration Example

```
2650-trm# show run
Building configuration...
Current configuration:
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2650-trm
!
boot system flash
!
!
!
memory-size iomem 20
voice-card 1
 ip subnet-zero
 no ip domain-lookup
 ip host dirt 223.255.254.254
 ip dhcp smart-relay
 !
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 mgcp modem passthrough voaal2 mode nse
 mgcp sdp simple
 mgcp default-package dt-package
 no mgcp timer receive-rtcp
 !
 !
 controller T1 0/0
 mode atm
  framing esf
 clock source internal
 linecode b8zs
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
 ds0-group 2 timeslots 2 type e&m-immediate-start
 ds0 busyout 24
```

```
!
!
!
!
interface FastEthernet0/0
 ip address 1.9.46.150 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface ATM0/0
 no ip address
 ip mroute-cache
 atm idle-cell-format itu
 atm uni-version 4.0
 atm voice aal2 aggregate-svc bandwidth 1500
 atm voice aal2 aggregate-svc traffic-parameters 1500 1500 65000
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa 222222222222.01 application aal2xgcp
 atm ilmi-keepalive
 pvc 0/5 qsaal
  !
 pvc 0/16 ilmi
  !
!
ip default-gateway 1.9.0.1
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 1.9.0.1
no ip http server
!
!
snmp-server engineID local 00000009020000024B1345A0
no snmp-server ifindex persist
snmp-server forwarder
snmp-server manager
!
voice-port 1/0:1
!
voice-port 1/0:2
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 1/0:1
 forward-digits all
!
dial-peer voice 2 pots
 application mgcpapp
 port 1/0:2
 forward-digits all
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
2650-trm#
```

MGCP PRI Backhaul Configuration Examples

Originating Gateway Configuration Example

```
2650-org# show run
Building configuration...
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2650-org
!
enable password lab
!
!
!
memory-size iomem 10
voice-card 1
 no ip subnet-zero
 no ip domain-lookup
 ip dhcp smart-relay
 !
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 mgcp modem passthrough voaal2 mode nse
 mgcp sdp simple
 mgcp default-package dt-package
 no mgcp timer receive-rtcp
 backhaul-session-manager
  set vsc2_set client nft
  group vsc2_grp set vsc2_set
  session group vsc2_grp 1.9.64.23 8004 1.9.46.170 8004 1
 isdn switch-type primary-5ess
 call rsvp-sync
 !
 !
 !
 controller T1 0/0
 mode atm
 framing esf
 clock source internal
 linecode b8zs
!
controller T1 0/1
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 1/1
!
!
!
!
interface Ethernet0/0
 ip address 1.9.46.170 255.255.0.0
 no cdp enable
!
interface Ethernet0/1
 no ip address
 shutdown
 no cdp enable
!
interface ATM0/0
```

```
 no ip address
 ip mroute-cache
 atm idle-cell-format itu
 atm uni-version 4.0
 atm voice aal2 aggregate-svc bandwidth 1500
 atm voice aal2 aggregate-svc traffic-parameters 1500 1500 65000
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa 111111111111.01 application aal2xgcp
 atm ilmi-keepalive
 pvc 0/5 qsaal
 !
 pvc 0/16 ilmi
 !
!
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-l3 backhaul vsc2_set
 no cdp enable
!
ip default-gateway 1.9.0.1
ip kerberos source-interface any
ip classless
no ip http server
!
no cdp run
!
snmp-server engineID local 000000090200005054747B80
no snmp-server ifindex persist
snmp-server forwarder
snmp-server manager
!
voice-port 1/0:23
!
dial-peer cor custom
!
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password lab
 login
!
no scheduler allocate
end
2650-org#
```

Terminating Gateway Configuration Example

```
2650-trm# show run
Building configuration...
Current configuration:
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2650-trm
!
boot system flash
!
```

```
!
!
memory-size iomem 20
voice-card 1
 ip subnet-zero
 no ip domain-lookup
 ip host dirt 223.255.254.254
 ip dhcp smart-relay
 !
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 mgcp modem passthrough voaal2 mode nse
 mgcp sdp simple
 mgcp default-package dt-package
 no mgcp timer receive-rtcp
 backhaul-session-manager
  set vsc1_set client nft
  group vsc1_grp set vsc1_set
  session group vsc1_grp 1.9.64.23 8000 1.9.46.150 8000 1
 isdn switch-type primary-5ess
 call rsvp-sync
 srcp 5555
 !
 !
 !
 !
 controller T1 0/0
 mode atm
 framing esf
 clock source internal
 linecode b8zs
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
!
!
!
!
interface FastEthernet0/0
 ip address 1.9.46.150 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface ATM0/0
 no ip address
 ip mroute-cache
 atm idle-cell-format itu
 atm uni-version 4.0
 atm voice aal2 aggregate-svc bandwidth 1500
 atm voice aal2 aggregate-svc traffic-parameters 1500 1500 65000
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa 222222222222.01 application aal2xgcp
 atm ilmi-keepalive
 pvc 0/5 qsaal
 !
 pvc 0/16 ilmi
 !
!
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
```

```
 isdn bind-l3 backhaul vsc1_set
 no cdp enable
!
ip default-gateway 1.9.0.1
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 1.9.0.1
no ip http server
!
!
snmp-server engineID local 00000009020000024B1345A0
no snmp-server ifindex persist
snmp-server forwarder
snmp-server manager
!
voice-port 1/0:23
!
dial-peer cor custom
!
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
no scheduler allocate
end
2650-trm#
```

Cisco 3660

MGCP CAS Call Examples

Originating Gateway Configuration Example

```
3660-org# show run
!
controller T1 3/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
!
interface ATM2/0
 ima-group 0
!
interface ATM2/1
 ima-group 0
!
interface ATM2/2
 ima-group 0
!
interface ATM2/3
 ima-group 0
!
interface ATM2/IMA0
 mtu 17998
 ip address 2.2.2.2 255.255.255.0
 pvc 65/100
  protocol ip 2.2.2.1 broadcast
```

```
  encapsulation aal5snap
 !
 pvc 65/101
  vbr-rt 1400 1400 60000
  vcci 2
  encapsulation aal2
 !
!
voice-port 3/0:1
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 3/0:1
!
!
end
```

Terminating Gateway Configuration Example

```
3660-trm# show run
memory-size iomem 30
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 no mgcp timer receive-rtcp
 isdn voice-call-failure 0
 call rsvp-sync
 !
 controller T1 1/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
!
interface ATM3/0
 ima-group 0
!
interface ATM3/1
 ima-group 0
!
interface ATM3/2
 ima-group 0
!
interface ATM3/3
 ima-group 0
!
interface ATM3/IMA0
 mtu 17998
 ip address 2.2.2.1 255.255.255.0
 pvc 65/100
  protocol ip 2.2.2.2 broadcast
  encapsulation aal5snap
 !
 pvc 65/101
  vbr-rt 1400 1400 60000
  vcci 2
  encapsulation aal2
 !
!
voice-port 1/0:1
!
dial-peer voice 1 pots
 application mgcpapp
 port 1/0:1
!
end
```

VoATM with AAL2 Trunking CAS Call Examples

Originating Gateway Configuration Example

```
3660-org# show run
!
controller T1 3/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
 ds0-group 2 timeslots 2 type e&m-immediate-start
!
interface ATM2/0
 ima-group 0
!
interface ATM2/1
 ima-group 0
 no scrambling-payload
!
interface ATM2/2
 ima-group 0
!
interface ATM2/3
 ima-group 0
!
interface ATM2/IMA0
 mtu 17998
 ip address 2.2.2.2 255.255.255.0
 pvc 65/100
  protocol ip 2.2.2.1 broadcast
  encapsulation aal5snap
 !
 pvc 65/101
  vbr-rt 1400 1400 60000
  vcci 2
  encapsulation aal2
 !
!
voice-port 3/0:1
 connection trunk 7200000
!
voice-port 3/0:2
 connection trunk 7200002
!
dial-peer voice 20 pots
 destination-pattern 7100000
 port 3/0:1
!
dial-peer voice 21 voatm
 destination-pattern 7200000
 session protocol aal2-trunk
 session target ATM2/IMA0 pvc 65/101 101
 signal-type trans
 codec aal2-profile ITUT 1 g711ulaw
 no vad
!
dial-peer voice 22 pots
 destination-pattern 7100002
 port 3/0:2
!
dial-peer voice 2003 voatm
 destination-pattern 7200002
 session protocol aal2-trunk
 session target ATM2/IMA0 pvc 65/101 102
 signal-type trans
 codec aal2-profile ITUT 1 g711ulaw
 no vad
```

```
!
!
end
```

Terminating Gateway Configuration Example

```
3660-trm# show run
memory-size iomem 30
 !
 controller T1 1/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
 ds0-group 2 timeslots 2 type e&m-immediate-start
!
interface ATM3/0
 ima-group 0
!
interface ATM3/1
 ima-group 0
!
interface ATM3/2
 ima-group 0
!
interface ATM3/3
 ima-group 0
!
interface ATM3/IMA0
 mtu 17998
 ip address 2.2.2.1 255.255.255.0
 pvc 65/100
  protocol ip 2.2.2.2 broadcast
  encapsulation aal5snap
 !
 pvc 65/101
  vbr-rt 1400 1400 60000
  vcci 2
  encapsulation aal2
 !
!
voice-port 1/0:1
 connection trunk 7200000
!
voice-port 1/0:2
 connection trunk 7200002
!
dial-peer voice 20 pots
 destination-pattern 7100000
 port 1/0:1
!
dial-peer voice 21 voatm
 destination-pattern 7200000
 session protocol aal2-trunk
 session target ATM3/IMA0 pvc 65/101 101
 signal-type trans
 codec aal2-profile ITUT 1 g711ulaw
 no vad
!
dial-peer voice 22 pots
 destination-pattern 7100002
 port 1/0:2
!
dial-peer voice 2002 voatm
 destination-pattern 7200002
 session protocol aal2-trunk
 session target ATM3/IMA0 pvc 65/101 102
 signal-type trans
 codec aal2-profile ITUT 1 g711ulaw
 no vad
```

```
!
end
```

VoATM with AAL2 Trunking CCS Call Examples

Originating Gateway Configuration Example

```
3660-org# show run
!
controller T1 3/0
 mode ccs frame-forwarding
 framing esf
 clock source internal
 linecode b8zs
 channel-group 23 timeslots 24 speed 64
 ds0-group 0 timeslots 1 type ext-sig
!
interface ATM2/1
 ima-group 0
!
interface ATM2/2
 ima-group 0
!
interface ATM2/3
 ima-group 0
!
interface ATM2/4
 ima-group 0
!
interface ATM2/IMA0
 mtu 17998
 ip address 2.2.2.1 255.255.255.0
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
 pvc 65/100
  protocol ip 2.2.2.2 broadcast
  encapsulation aal5snap
 !
 pvc 65/101
  vbr-rt 500 500 500
  encapsulation aal2
 !
 pvc 65/102
  vbr-rt 500 500 500
  encapsulation aal5mux voice
 !
!
interface Serial3/0:23
 no ip address
 no keepalive
 ccs encap atm
 ccs connect ATM2/IMA0 pvc 65/102
!
voice-port 3/0:0
 connection trunk 2000
!
dial-peer cor custom
!
!
!
dial-peer voice 1000 pots
 destination-pattern 1000
 port 3/0:0
!
dial-peer voice 2000 voatm
 destination-pattern 2000
 called-number 1000
 session protocol aal2-trunk
```

```
 session target ATM2/IMA0 pvc 65/101 100
 signal-type ext-signal
 codec aal2-profile ITUT 1 g711ulaw
 no vad
!
!
end
```

Terminating Gateway Configuration Example

```
3660-trm# show run
!
 controller T1 1/0
 mode ccs frame-forwarding
 framing esf
 clock source internal
 linecode b8zs
 channel-group 23 timeslots 24 speed 64
 ds0-group 0 timeslots 1 type ext-sig
!
interface Serial1/0:23
 no ip address
 no keepalive
 ccs encap atm
 ccs connect ATM3/IMA0 pvc 65/102
!
interface ATM3/0
 ima-group 0
!
interface ATM3/IMA0
 mtu 17998
 ip address 2.2.2.2 255.255.255.0
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
 pvc 65/100
  protocol ip 2.2.2.1 broadcast
  encapsulation aal5snap
 !
 pvc 65/101
  vbr-rt 500 500 500
  encapsulation aal2
 !
 pvc 65/102
  vbr-rt 500 500 500
  encapsulation aal5mux voice
 !
!
!
voice-port 1/0:0
 connection trunk 2000
!
dial-peer voice 1000 pots
 destination-pattern 1000
 port 1/0:0
!
dial-peer voice 2000 voatm
 destination-pattern 2000
 called-number 1000
 session protocol aal2-trunk
 session target ATM3/IMA0 pvc 65/101 100
 signal-type ext-signal
 codec aal2-profile ITUT 1 g711ulaw
 no vad
!
!
end
```

PRI Q.931 Signaling Backhaul Examples

Originating Gateway Configuration Example

```
3660-org# show run
memory-size iomem 30
 !
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 mgcp modem passthrough voaal2 mode nse
 mgcp sdp simple
 mgcp default-package dt-package
 no mgcp timer receive-rtcp
 backhaul-session-manager
   set vsc1_set client nft
   group vsc1_grp set vsc1_set
   session group vsc1_grp 1.9.64.23 8004 1.9.47.55 8004 1
 isdn switch-type primary-5ess
 isdn voice-call-failure 0
 call rsvp-sync
 !
 voice class codec 1
!
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-l3 backhaul vsc1_set
 no cdp enable
!
interface ATM2/0
 ima-group 0
!
interface ATM2/1
 ima-group 0
!
interface ATM2/2
 ima-group 0
!
interface ATM2/3
 ima-group 0
!
interface ATM2/IMA0
 mtu 17998
 ip address 2.2.2.2 255.255.255.0
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc bandwidth 1536
 atm voice aal2 aggregate-svc traffic-parameters 1536 1536 65536
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa AAAAAAAAAAAA.01 application aal2xgcp
 pvc 0/5 qsaal
 !
 pvc 0/16 ilmi
 !
 pvc 65/100
  protocol ip 2.2.2.1 broadcast
  encapsulation aal5snap
 !
 pvc 65/101
```

```
  vbr-rt 1400 1400 60000
  vcci 2
  encapsulation aal2
 !
!
voice-port 1/0:23
!
dial-peer voice 1 pots
 application mgcpapp
 forward-digits all
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 transport input none
line aux 0
line vty 0 4
 login
!
scheduler allocate 5000 3000
end
```

Terminating Gateway Configuration Example

```
3660-trm# show run
!
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 mgcp modem passthrough voaal2 mode nse
 mgcp sdp simple
 mgcp default-package dt-package
 no mgcp timer receive-rtcp
 backhaul-session-manager
   set vsc1_set client nft
   group vsc1_grp set vsc1_set
   session group vsc1_grp 1.9.64.23 8000 1.9.48.41 8000 1
 isdn switch-type primary-5ess
 isdn voice-call-failure 0
 call rsvp-sync
 !
 !
 !
 !
 !
 !
 !
 controller T1 1/0
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
interface Serial1/0:23
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn bind-l3 backhaul vsc1_set
!
interface ATM3/0
 ima-group 0
!
interface ATM3/1
 ima-group 0
!
interface ATM3/2
 ima-group 0
```

```
!
interface ATM3/3
 ima-group 0
!
interface ATM3/IMA0
 mtu 17998
 ip address 2.2.2.1 255.255.255.0
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc bandwidth 1536
 atm voice aal2 aggregate-svc traffic-parameters 1536 1536 65536
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa 999999999999.01 application aal2xgcp
 pvc 0/5 qsaal
 !
 pvc 0/16 ilmi
 !
 pvc 65/100
  protocol ip 2.2.2.2 broadcast
  encapsulation aal5snap
 !
 pvc 65/101
  vbr-rt 1400 1400 60000
  vcci 2
  encapsulation aal2
 !
!
voice-port 1/0:23
!
dial-peer voice 1 pots
 application mgcpapp
!
!
end
```

PRI Q.931 Signaling Backhaul CAS Call Examples

Originating Gateway Configuration Example

```
3660-org# show run
memory-size iomem 30
 !
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 mgcp modem passthrough voaal2 mode nse
 no mgcp timer receive-rtcp
 call rsvp-sync
 !
 voice class codec 1
!
!
!
!
!
!
!
controller T1 3/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
!
interface ATM2/0
 ima-group 0
!
interface ATM2/1
 ima-group 0
!
interface ATM2/2
```

```
 ima-group 0
!
interface ATM2/3
 ima-group 0
!
interface ATM2/IMA0
 mtu 17998
 ip address 2.2.2.2 255.255.255.0
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc bandwidth 1536
 atm voice aal2 aggregate-svc traffic-parameters 1536 1536 65536
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa AAAAAAAAAAAA.01 application aal2xgcp
 pvc 0/5 qsaal
 !
 pvc 0/16 ilmi
 !
 pvc 65/100
  protocol ip 2.2.2.1 broadcast
  encapsulation aal5snap
 !
!
voice-port 3/0:1
!
dial-peer voice 1 pots
 application mgcpapp
 port 3/0:1
 forward-digits all
!
end
```

Terminating Gateway Configuration Example

```
3660-trm# show run
!
 mgcp
 mgcp call-agent 1.9.64.23 service-type mgcp version 0.1
 mgcp modem passthrough voaal2 mode nse
 no mgcp timer receive-rtcp
 isdn voice-call-failure 0
 call rsvp-sync
 !
 controller T1 1/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-immediate-start
!
interface ATM3/0
 ima-group 0
!
interface ATM3/1
 ima-group 0
!
interface ATM3/2
 ima-group 0
!
interface ATM3/3
 ima-group 0
!
interface ATM3/IMA0
 mtu 17998
 ip address 2.2.2.1 255.255.255.0
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc bandwidth 1536
 atm voice aal2 aggregate-svc traffic-parameters 1536 1536 65536
 atm voice aal2 aggregate-svc upspeed-number 100
 atm voice aesa 999999999999.01 application aal2xgcp
 pvc 0/5 qsaal
 !
```

```
 pvc 0/16 ilmi
 !
 pvc 65/100
  protocol ip 2.2.2.2 broadcast
  encapsulation aal5snap
 !
!
voice-port 1/0:1
!
dial-peer voice 1 pots
 application mgcpapp
 port 1/0:1
!
end
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Asynchronous Transfer Mode Command Reference*. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **vbd-playout-delay maximum**
- **vbd-playout-delay minimum**
- **vbd-playout-delay mode**
- **vbd-playout-delay nominal**
- **subcell-mux**

Glossary

inform --SNMP trap message that includes a delivery confirmation request.

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

NMS --Network Management System. An application or suite of applications designed to monitor networks using SNMP. CiscoView is one example of an NMS.

OAM --Operation, Administration, and Maintenance. ATM Forum specifies OAM cells used to monitor virtual circuits. OAM cells provide a virtual circuit-level loopback in which a router responds to the cells, demonstrating that the circuit is up and the router is operational.

PVC --Permanent Virtual Circuit. Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, PVC also stands for permanent virtual connection.

SNMP --Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents and is exclusively used in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

trap --A message from an SNMP agent alerting the SNMP manager to a condition on the network.

VCI --Virtual Channel Identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next network VCL that a cell needs to transit on its way to its final destination.

VCL --Virtual Channel Link. Connection between two ATM devices.

VPI --Virtual Path Identifier. Eight-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next VCL that a cell needs to transit on its way to its final destination. The function of the VPI is similar to that of the DLCI in Frame Relay.

CHAPTER 12

Unspecified Bit Rate Plus and ATM Enhancements

Feature History

Release	Modification
12.2(2)XB	The UBR+ and ATM Enhancements for Service Provider Integrated Access feature was introduced for the Cisco 2600 series and Cisco MC3810.
12.2(8)T	This feature was integrated into the Cisco IOS Release 12.2(8)T

This document describes the Unspecified Bit Rate plus (UBR+) and ATM Enhancements for Service Provider (SP) Integrated Access feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

The UBR+ and ATM Enhancements for SP Integrated Access feature includes the following:

- UBR+ functionality
- Proportional allocation of excess bandwidth
- Oversubscription of the Cisco MC3810-MFT T1/E1 trunk and similar ATM-capable VWIC-1MFT-E1 and VWIC-1MFT-T1 interfaces offered on the Cisco 2600 series

Note This feature is not supported on the UBR+ and ATM Enhancements for SP Integrated Access non-VWIC WICs.

These enhancements permit the oversubscription of ATM trunks for UBR+ permanent virtual circuits (PVCs).

UBR+ supports a zero committed information rate (CIR) with infinite burst capabilities up to an entire T1/E1. It allows any available network bandwidth to be continuously usable by any data application. For this feature, all data traffic in the network uses UBR+ end to end. The zero CIR with infinite burst feature is exclusive to data traffic and is implemented for AAL5 only.

When UBR CPE to ATM switch (not the UBR+ and ATM Enhancements for SP Integrated Access feature) is configured, a file transfer from one virtual circuit (VC) utilizes the entire trunk bandwidth when no other VCs (data or voice) are active. When other VCs become active with fixed CIRs, because UBR+ is not configured, the new VCs are not guaranteed their intended CIR. UBR+ resolves this by reallocating the configured CIRs to guarantee that all VCs achieve the appropriate throughput. If there is any remaining bandwidth, bursting up to that availability is still permitted.

Because UBR allows for a continuous burst, bandwidth could be conserved by assigning a UBR class of service (CoS) to the VC. However, UBR has a variable bit rate (VBR) that constrains the burst period to a maximum burst size (MBS), rather than allowing a continuous burst. The UBR+ and ATM Enhancements for SP Integrated Access feature does not have an MBS constraint.

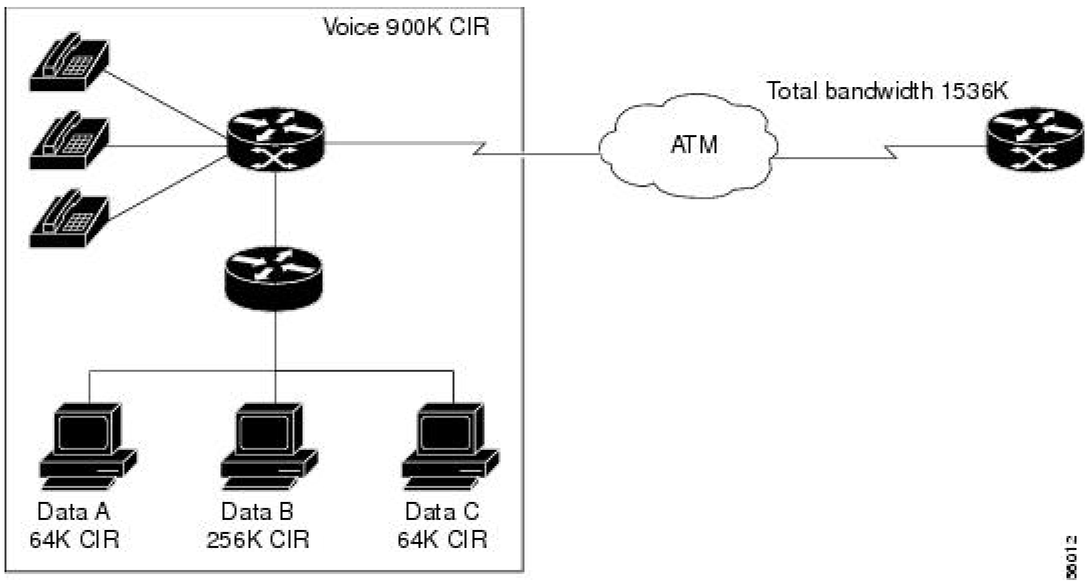
Policing and Shaping for Guaranteed Bandwidth

In addition to allowing data applications to burst without limitation up to entire T1/E1, a guaranteed minimum bandwidth per virtual circuit (VC) should be permitted for UBR sessions to ensure that the bandwidth of all

UBR+ VCs are equal to their relative configured minimum cell rate (MCR). Each VC should be able to have a defined amount of guaranteed bandwidth. The UBR+ and ATM Enhancements for SP Integrated Access feature supports a maximum total ATM bandwidth of 1536K on an ATM trunk. Many different configurations are allowable, such as the one shown in the figure below.

Note The policing and shaping for the guaranteed bandwidth enhancement is exclusive to UBR data traffic and is implemented for AAL5.

Figure 15: For UBR+ the Maximum Total ATM Bandwidth on an ATM Trunk Is 1536K



The table shown in the figure below shows the offered load and allocated bandwidth for three VCs using UBR+ called Data A, Data B, and Data C. During time 0 to time 2, there is no voice traffic and bandwidth is allocated for the three VCs as each requires. During time 3 to time 5, the voice VC carries traffic of 900 Kbps. Because voice traffic has a higher precedence over data traffic, 900 Kbps out of a total of 1536 Kbps are reserved for voice. The remaining 636 Kbps are shared by Data A, Data B, and Data C.

Bandwidth sharing begins with an allotment of CIRs to the individual data VCs. This is reflected in the Data A, Data B, and Data C "allocated bandwidth" columns in the figure below. Depending on the offered load, each event shows either the CIR or the total CIR and free bandwidth for the data VC. Next, the excess bandwidth is computed by subtracting the sum of CIRs of data VCs from 636 Kbps. The excess bandwidth is then equally shared by all of the data VCs that are carrying traffic.

Figure 16: Offered Load and Allocated Load with and Without Voice Traffic

		UBR+		UBR+		UBR+							
Event		Data A		Data B		Data C		total Data		Voice		Total	
	CIR	64		256		64		384		900		1284	
		offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w
file transfer	time=0	1536	1536	0	0	0	0	1536	1536	0	0	1536	1536
inventory update	time=1	1280	1280	256	256	0	0	1536	1536	0	0	1536	1536
credit auth	time=2	1216	1216	256	256	64	64	1536	1536	0	0	1536	1536
20 G.726 calls	time=3	1172	316	256	256	64	64	1492	636	900	900	2392	1536
proporational share	time=4	960	190	512	382	64	64	1536	636	900	900	2436	1536
credit auth stops	time=5	992	222	544	414	0	0	1536	636	900	900	2436	1536

Each event time unit is described in further detail below:

Table 13: Time Event Table for Offered and Allocated Loads with and Without Voice Traffic

Time	Event
Time = 0	A file transfer occurs across VC A and occupies all trunk bandwidth. The VC is only guaranteed 64 Kbps, but because there is no competing traffic and the VC is allowed to burst, all of 1536K trunk bandwidth is allocated to VC A. Note that because VC A is a UBR+ circuit, it has a CIR.
Time = 1	In addition to the file transfer, an inventory update application occurs across VC B. The inventory application requires 256K and the VC is guaranteed 256K. In this case, the external router throttles the file transfer VC. Because the total offered load does not exceed the trunk bandwidth, the VCs are serviced at their offered load.
Time = 2	A credit authorization application occurs across VCC and uses 64 Kbps. Again, the external router throttles the offered load to fit within the trunk bandwidth. At this point, all offered loads are allocated.

Time	Event
Time = 3	Twenty G.726 voice calls are initiated and use 900K. The external router is still offering 1536K. The combined data and voice offered load cannot fit across the ATM trunk, so the access device must throttle and shape the offered data load. Because Data B and Data C are offering load at their committed rate, they are not throttled. Data A is bursting above its minimum, and its throughput reduces to accommodate the voice load. At this point, a typical TCP/IP file transfer would throttle back to the delivered throughput, but the traffic might also be a User Datagram Protocol (UDP) stream that might not throttle back and instead offer a continuous load.
Time = 4	The inventory update application begins to offer more than 256 Kbps of load. The external router prioritizes the inventory application and adjusts its queuing. At this point, multiple PVCs are competing for excess unsubscribed bandwidth. There are only 252 Kbps of unsubscribed bandwidth, and it is allocated on a round-robin basis. Because two PVCs are competing for the excess bandwidth, they each get half of the excess. Each bursting PVC's throughput is its CIR plus half of the unsubscribed bandwidth. Data A gets 64K and 126K, for a total of 190K. Data B gets 256K and 126K, for a total of 382K.
Time = 5	The credit authorization application stops. The 64K bandwidth it was using goes back to the unsubscribed or unallocated pool, and is r-allocated to the bursting PVCs. Again, the allocation is round-robin, so Data A and Data B get another 32K each.

Fair Sharing of Unsubscribed and Non-Allocated Bandwidth

In addition to guaranteeing a minimum rate while allowing unlimited bursting, control over how excess bandwidth is applied to bursting PVCs must be exercised. Without the fair sharing of unsubscribed and unused bandwidth, bandwidth is allocated to bursting PVCs on a round-robin basis. PVCs are serviced at their minimum rate, and a traffic-shaping algorithm provides cells to each bursting PVC in sequence.

With the UBR+ and ATM Enhancements for SP Integrated Access feature, a weight is used for the allocation of bursting cells that is based on the CIR of each PVC. This fair sharing of unsubscribed bandwidth is applicable to AAL5-based data traffic.

The table in the figure below is essentially the same as the table in "Policing and Shaping for Guaranteed Bandwidth" section. The difference is the manner in which data VCs share excess bandwidth. Excess bandwidth is not shared equally among competing traffic. Instead, it is shared in proportion to the CIRs of the VCs. For example, if Data A has a CIR of 64 Kbps and Data B has a CIR of 256 Kbps, and there is 252 Kbps excess bandwidth, then the excess bandwidth is shared 1:4 by the Data A and Data B VCs. Therefore, Data A is allocated 51 Kbps, and Data B is allocated 201 Kbps.

This application could still be addressed with constant bit rate plus (CBR+) CoS assigned to the PVCs. However, a special implementation of the traffic shaping algorithm would be responsible for the fair weighted allocation of unsubscribed and unused bandwidth to the bursting PVCs.

Note With a lower CIR, Data A in the table in the figure below receives proportionally less bandwidth than Data B. Variable Bit Rate real time (VBRrt) class Voice receives all the bandwidth required.

Figure 17: Offered Load and Allocated Load with Excess Bandwidth Shared in Proportion to the CIRs of the VCs

		UBR+		UBR+									
Event		Data A		Data B		Data C		total Data		Voice		Total	
	CIR	64		256		64		384		900		1284	
		offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocate b/w
file transfer	time=0	1536	1536	0	0	0	0	1536	1536	0	0	1536	153
inventory update	time=1	1280	1280	256	256	0	0	1536	1536	0	0	1536	153
credit auth	time=2	1216	1216	256	256	64	64	1536	1536	0	0	1536	153
20 G.726 calls	time=3	1216	316	256	256	64	64	1536	636	900	900	2436	153
proporational share	time=4	960	115	512	457	64	64	1536	636	900	900	2436	153
credit auth stops	time=5	992	128	544	508	0	0	1536	636	900	900	2436	153

Each event time unit is described in further detail below:

Table 14: Time Event Table for Offered and Allocated Loads with Excess Bandwidth

Time	Event
Time = 0, 1, 2, 3	While only one PVC is bursting, it gets all remaining bandwidth.
Time = 4	Two PVC's (Data A and Data B) are bursting. The unsubscribed and unused bandwidth is shared among them with respect to their CIR. There is 252 Kbps of unsubscribed bandwidth. Data B gets four times as much of that excess bandwidth as does Data A. So Data B gets an additional 201K and Data A gets an additional 51K.
Time = 5	After the PVCs are serviced at their minimum rate, 316K of unsubscribed and unused bandwidth is available. So Data B gets 252K and Data A gets 64K of additional bandwidth.

Oversubscription of WAN Uplink

Another element to consider is the oversubscription of the Frame Relay service. The intent of all oversubscription schemes is to assign a relative ranking between PVCs that are offering load. If all PVCs offer load, then their allocated bandwidths reflect their relative CIRs, even if they cannot be met. If there is a mix of PVCs offering load and PVCs not offering load, then the relative committed rates of the PVCs not offering load are sustained.

In the table in the figure below, the cumulative CIR of the VCs' exceed line rate is 1536 Kbps. However, the total bandwidth of the WAN link cannot exceed the line rate of 1536 Kbps. If all the VCs are carrying load and the data VCs cannot get bandwidth equal to their CIR, then the bandwidth allotted to the data VCs will be reduced relative to their CIR values.

The implementation of the oversubscription of the WAN uplink is configurable on a per-VC basis and is applicable to voice (VBRrt, CBR/AAL2) and data (UBR, UBR+, CBR, Variable Bit Rate non real time (VBRnrt)/AAL5) traffic.

Note For the UBR+ and ATM Enhancements for SP Integrated Access feature, voice VC is allotted 900 Kbps, and the total available bandwidth of the WAN uplink can never be exceeded.

Figure 18: Offered Load and Allocated Load with Oversubscription Frame Relay

		UBR+		UBR+		UBR+							
Event		Data A		Data B		Data C		total Data		Voice		Total	
	CIR	64		256		512		832		900		1732	
		offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allocated b/w	offered load	allo b
file transfer	time=0	1536	1536	0	0	0	0	1536	1536	0	0	1536	
inventory update	time=1	1280	1280	256	256	0	0	1536	1536	0	0	1536	
credit auth	time=2	1216	1216	256	256	64	64	1536	1536	0	0	1536	
20 G.726 calls	time=3	1172	316	256	256	64	64	1492	636	900	900	2392	
proporational share	time=4	960	115	512	457	64	64	1536	636	900	900	2436	
credit auth stops	time=5	992	128	544	508	0	0	1536	636	900	900	2436	
inventory ends/credit increases	time=6	1024	124	0	0	512	512	1536	636	900	900	2436	
credit bursts above CIR	time=7	768	70	0	0	768	566	1536	636	900	900	2436	
all pvc burst	time=8	384	48	384	196	768	392	1536	636	900	900	2436	

Each event time unit is described in further detail below:

Table 15: Time Event Table for Offered and Allocated Loads with Oversubscription Frame Relay

Time	Event
Time = 0, 1, 2, 3, 4, 5	The same conditions as previously described exist. The guaranteed minimums are oversubscribed, but because Data C is offering load at much less than its CIR, all PVCs are serviced by at least their CIRs, and unused bandwidth is "fairly weighted" among the bursting PVCs. Because Data B has a higher CIR, it gets more of the unused bandwidth than Data A does.9
Time = 6	The inventory update application ends, and the credit authorization application increases its offered load to 512K. At this point, each PVC can be serviced at its CIR. Only Data A PVC is bursting, and it gets the unused bandwidth. If Data C PVC had been provisioned without oversubscription, it would have been assigned 316K and would have been allocated unused bandwidth at five times the rate of Data A.
Time = 7	The credit authorization bursts above its CIR and takes excess bandwidth from Data A.
Time = 8	All data PVCs are bursting above their CIR, and the combined CIR cannot be met. The voice PVC is serviced first because it is a higher class of service (VBRrt versus UBR+). When the voice PVC is serviced, 636K of bandwidth has to be shared by data PVCs with a combined CIR of 832K. Because the CIR minimum cannot be met, the PVCs are serviced at a rate that reflects their relative CIRs.

Benefits

- Provides unique class of service (CoS) categories for service product differentiation
- Optimizes excess bandwidth
- Permits overprovisioning and oversubscription of available bandwidth
- Provides ATM as a WAN technology. Among the many fundamental benefits of deploying ATM and its applications in a WAN are:
    - Advanced statistical multiplexing
    - Bandwidth optimization
    - Multiservice traffic aggregation

Restrictions

This feature must be used with the ATM software segmentation and reassembly (SAR) feature. It cannot be ported to the following interfaces:

- ATM SAR Advanced Integration Module (AIM)
- SAR and Digital Signal Processor (DSP) AIM
- Multiport T1/E1 ATM network modules with inverse multiplexing over ATM on Cisco 2600 and Cisco 3600 series routers
- ATM OC-3 network module for Cisco 3600 series routers
- Cisco IOS release 12.2(2)XB or higher

Related Features and Technologies

ATM segmentation and reassembly (SAR)

Related Documents

- *ATM Segmentation and Reassembly (SAR)*
- Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2
- Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2
- Cisco IOS Interface Command Reference, Release 12.2
- Cisco IOS Interface Configuration Guide, Release 12.2

Supported Platforms

- Cisco 2600 series
- Cisco MC3810

Supported Standards and MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Before you enable PVC trap support, you must configure SNMP support and an IP routing protocol on your router. See the "ATM Configuration Examples" section.

For more information about configuring SNMP support, refer to the chapter "Configuring SNMP Support" in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about configuring IP routing protocols, refer to the *Cisco IOS IP Routing Protocols Configuration Guide*.

To receive PVC failure notification and access to PVC status tables on your router, you must have the Cisco PVC trap MIB called CISCO-IETF-ATM2-PVCTRAP-MIB.my compiled in your NMS application. You can find this MIB on the Web at Cisco's MIB websiteat the URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Configuration Tasks

Configuring UBR Plus PVCs

SUMMARY STEPS

1. Router(config)# **interface atm0** [*subinterface-number* [**multipoint** | **point-to-point**]]
2. Router(config-subif)# **pvc** *name vpi/vci*[**ilmi**| **qsaal**| **smds**]
3. Router(config-if-atm-vc)# **ubr+** *output-pcr output-mcr*[*input-pcr*] [*input-mcr*]
4. Router(config-if-atm-vc)# **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm0** [*subinterface-number* [**multipoint** | **point-to-point**]]	Enters interface configuration mode to configure ATM interface or an ATM subinterface, such as 0/0.1. The default for subinterfaces is **multipoint.**
Step 2	Router(config-subif)# **pvc** *name vpi/vci*[**ilmi**| **qsaal**| **smds**]	Creates a signaling PVC that carries signaling to establish an switched virtual circuit (SVC). For example: Router(config-if)# **pvc atm1 100/100**

	Command or Action	Purpose
		The arguments for this command have the following meanings: *name --(Optional)* The name of the PVC or map. The name can be up to 16 characters long. *vpi/* --ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a vpi value defaults the vpi value to 0. The arguments vpi and vci cannot both be set to 0; if one is 0, the other cannot be 0. *vci* --ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. Typically, lower values 0 to 31 are reserved for specific traffic (for example, F4 OAM, SVC signaling, Interim Local Management Interface (ILMI), and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link--not throughout the ATM network--because it has local significance only. The arguments vpi and vci cannot both be set to 0; if one is 0, the other cannot be 0. **ilmi** --*(Optional)* Used to set up communication with the ILMI; the associated vpi and vci values ordinarily are 0 and 16, respectively. **qsaal** --*(Optional)* A signaling-type PVC used for setting up or tearing down SVCs; the associated vpi and vci values ordinarily are 0 and 5, respectively.
Step 3	Router(config-if-atm-vc)# **ubr+** *output-pcr output-mcr*[*input-pcr*] [*input-mcr*]	Specifies the output peak cell rate (PCR) and output guaranteed minimum cell rate (MCR) for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle member.
Step 4	Router(config-if-atm-vc)# **no shutdown**	Ensures that interface is activated.

Verifying the Addition of the UBR Plus PVC

To verify that the UBR+ PVC was created use the **show atm pvc** command. The following is an example output:

```
Router# show atm pvc
VCD/
Interface Name VPI VCI Type Encaps SC   Kbps Kbps Cells Sts
0/0.1     atm1 100 100 PVC  SNAP   UBR+ 1536 786  UP    ( 786)
```

Note The PVC is added with 768 Kbps of guaranteed bandwidth.

Troubleshooting Tips

To troubleshoot the ATM and IMA group configuration, enter the **ping** command, which checks host reachability and network connectivity. This command can confirm basic network connectivity on the AppleTalk, ISO CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks.

For IP, the **ping** command sends ICMP (Internet Control Message Protocol) Echo messages. If a station receives an ICMP Echo message, it sends an ICMP Echo Reply message back to the source.

The extended command mode of the **ping** command permits you to specify the supported IP header options so that the router can perform a more extensive range of test options. To enter **ping** extended command mode, enter **yes** at the "extended commands" prompt of the **ping** command.

For detailed information on using the **ping** and extended **ping** commands, see the *Cisco IOS Configuration Fundamentals Command Reference*.

If a **ping** command fails, check the following possible reasons for the connectivity problem:

- The interface is down, causing a "no ip route" error message.
- The PVC or SVC does not include proper mapping configured for the destination address, causing an "encapsulation failure" error. For more information about configuring encapsulation, see the section "Configuring IMA Groups, on page 65" earlier in this chapter and the **encapsulation aal5** command in the *Cisco IOS Asynchronous Transfer Mode Command Reference*.
- If there is a firmware problem, the **show controller atm**command shows whether an interface is able to transmit and receive cells. For sample output, see the earlier section "Verifying an ATM Interface Configured for IMA Operation, on page 61."

Tip Use the **ping** command when the network is functioning properly to see how the command works under normal conditions and so to compare the results when troubleshooting.

If a communication session is closing when it should not be, an end-to-end connection problem can be the cause. The **debug ip packet** command is useful for analyzing the messages traveling between the local and remote hosts. IP debugging information includes packets received, generated, and forwarded. Because the **debug ip packet** command generates a significant amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

Monitoring and Maintaining the UBR Plus VCs

The following **show**and **clear**commands are used to monitor and maintain UBR+ VCs:

Command	Purpose
Router# **show atm pvc** [*vpi*/*vci* | *name* | **interface atm** *interface-number*]	Displays all ATM permanent virtual circuits (PVCs) and traffic information. Note that *vpi/vci* is the *vpi/vci* of the UBR+ VC.
Router# **clear counters** [*type*]	Clears statistics on all the VCs that have been configured.

Configuration Examples

show run Command Example

The following is output from a **show run** command on a Cisco MC3810 router:

```
Router# show run
Current configuration :73 bytes
!
interface ATM0.1 multipoint
 pvc atm1 101/101
  ubr+ 1536 768
!
end
```

show atm pvc Command Example

The following is output from a show **atm pvc command on** a Cisco MC3810 router:

```
Router# sh atm pvc
            VCD /                                          Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC    Kbps   Kbps   Cells  Sts
0.1        atm1       101   101   PVC    SNAP     UBR+   1536    768          UP (   768)
```

show atm pvc Command Example

The following is output from a show **atm pvc 101/101**on a Cisco MC3810 router:

```
Router# show atm pvc 101/101
ATM0.1: VCf: 131, VPI: 101, VCI: 101, Connection Name: atm1
UBR+, PeakRate: 1536, Minimum Guaranteed Rate: 768
AAL5-LLC/SNAP, etype:0x0, Flags: 0x20, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not Managed
```

Command Reference

No new commands were introduced with this feature. All the commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

For further information on related documentation, see the "Related Documents" section.

Glossary

AAL-- ATM adaptation layer. The standards layer that allows multiple applications to have data converted to and from the ATM call. A protocol used that translates higher layer services into the size and format of an ATM cell. ATM Adaptation Layer sits above ATM and converts non-ATM bit streams - end user data - into ATM cells. The AAL accepts data from different applications and presents it to the ATM layer in the form of 48-byte ATM payload segments. AALs consist of two sublayers: CS and SAR. The AAL is the protocol used on top of ATM to support higher-layer service requirements. For data communications services, the AAL defines a segmentation/re-assembly protocol for mapping large data packets into the 48-octet payload field of an ATM cell. AALs differ on the basis of the source-destination timing used, whether they use CBR or VBR, and whether they are used for connection-oriented or connectionless mode data transfer. At present, the four types of AAL recommended by the ITU-T are AAL1, AAL2, AAL3/4, and AAL5.

AAL2 --ATM adaptation layer 2. One of four AALs recommended by the ITU-T. AAL2 is used for connection-oriented services that support a variable bit rate, such as some isochronous video and voice traffic. See also AAL and ATM.

AAL5 --ATM adaptation layer 5. One of four AALs recommended by the ITU-T. AAL5 supports connection-oriented VBR services and is used predominantly for the transfer of classical IP over ATM and LANE traffic. AAL5 uses SEAL and is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability. See also AAL, ATM, and SEAL.

ACR-- 1. actual cell rate. The rate at which the source is transmitting cells in an asynchronous transfer mode (ATM) available bit rate (ABR) connection. 2. allowed cell rate: An ABR service parameter, ACR is the current rate, in cells/sec, at which the source is allowed to transmit cells in an asynchronous transfer mode (ATM) available bit rate (ABR) connection. In other words, the available bandwidth, in cells per seconds, for a given quality of service (QoS) class, which is dynamically controlled by the network.

ATM --Asynchronous Transfer Mode. International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E2, SONET, and T3.

CBR--constant bit rate. QoS class defined by the ATM forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery.

CIR --committed information rate. In a Frame Relay network, each PVC is assigned a Committed Information Rate, measured in bits per second. The CIR represents the average capacity that the Port Connection should allocate to the PVC. This rate should be consistent with the expected average traffic volume between the two sites that the PVC connects. The CIR that is assigned to a PVC cannot exceed the speed of either the originating or terminating Port Connection. The rate is averaged over a minimum increment of time.

CoS --class of service. Telephone service distinctions that include rate differences between individual and party lines, flat rate and message rate, and restricted and extended area service.

CS--convergence sublayer. One of the two sublayers of the AAL common part convergence sublayer (CPCS), which is responsible for padding and error-checking. PDUs passed from the SSCS are appended with an 8-byte trailer (for error checking and other control information) and padded, if necessary so that the protocol data unit (PDU) is divisible by 48. These PDUs are then passed to the SAR sublayer of the CPCS for further processing. See also AAL, and SAR.

ELAN--emulated LAN. ATM network in which an Ethernet or Token ring LAN is emulated using a client-server model. Multiple ELANs can exist simultaneously on a single ATM network. ELANS are defined by the LANE specification.

LAN--local area network.

LANE--LAN emulation. Technology that allows an ATM network to function as a LAN backbone. The ATM network must provide multicast and broadcast support, address mapping (MAC-to-ATM), SVC management, and a usable packet format. LANE also defines Ethernet and Token Ring ELANs.

maximum burst --Specifies the largest burst of data above the insured rate that is allowed temporarily on an ATM PVC, but is not dropped at the edge by the traffic policing function--even if it exceeds the maximum rate. This amount of traffic is allowed only temporarily; in general, the traffic source needs to be within the maximum rate. Specified in bytes or cells.

MBS --maximum burst size. See maximum burst.

MCR --minimum cell rate. ATM term for an ABR (Available Bit Rate) service traffic descriptor, in cells/sec, that is the rate at which the source is always allowed to send. This parameter is defined by the ATM Forum for ATM traffic management. MCR is defined only for ABR transmissions, and specifies the minimum value for the ACR. See ACR.

PCR --peak cell rate. Parameter defined by The ATM Forum for ATM traffic management. In CBR transmissions, PCR determines how often data samples are sent. In ABR transmissions, PCR determines the maximum value of the ACR. See ACR.

PVC --permanent virtual circuit. A circuit or channel through an ATM network provisioned by a carrier between two endpoints; used for dedicated long-term information transport between locations. Also virtual connection (VPC/ VCC) provisioned for indefinite use in an ATM network, established by the network management system (NMS). This is a link with static route defined in advance, usually by manual setup. Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. Called a permanent virtual connection in ATM terminology. Compare with SVC.

SEAL--simple and efficient AAL. Scheme used by AAL5 in which the SAR sublayer segments CS protocol data units without adding additional fields. See AAL, AAL5, CS, and SAR.

SVC --switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic.

UBR --unspecified bit rate. Traffic class defined by the ATM Forum. UBR is an ATM service category that does not specify traffic related service guarantees. UBR allows any amount of data up to a specified maximum to be sent across the network, but there are no guarantees in terms of cell loss rate and delay. Specifically, UBR does not include the notion of a per-connection negotiated bandwidth. No numerical commitments are made with respect to the cell loss ratio experienced by a UBR connection, or as to the cell transfer delay experienced by cells on the connection.

UBR+ --UBR with early packet discard (EPD) or partial packet discard (PPD).

VCC --virtual channel connection. As an ATM term, it is a concatenation of VCLs that extends between the points where the ATM service users access the ATM layer. The points at which the ATM cell payload is passed to, or received from, the users of the ATM Layer (that is, a higher layer or ATM entity) for processing signify the endpoints of a VCC. VCCs are unidirectional. ATM VCC can have one of two services types: 1) connection-oriented-path established before data is sent or 2) Connectionless data sent as datagrams. The connection-oriented path is typically used for AAL 1, 2, 3, 5 circuits. The connectionless VCC is for AAL4 is usually associated with Switched Multimegabit Data Service (SMDS).

VCL --virtual channel link. A means of unidirectional transport of ATM cells between the point where a VCI value is assigned and the point where that value is translated or removed.

CHAPTER 13

Enhanced Voice and QoS for ADSL and G.SHDSL

QoS features make it possible to effectively combine voice and data traffic in the same WAN connection without sacrificing quality and reliability. Service providers can increase revenue by building differentiated service options based on premium, standard, or best-effort service classes.

This document describes enhancements to the voice and quality of service (QoS) features for asymmetric digital subscriber lines (ADSLs) and single-pair high-bit-rate digital subscriber lines (G.SHDSLs). When the ADSL or G.SHDSL WAN interface cards (WICs) are installed, they support the integration of voice and data over the same ADSL or G.SHDSL circuit using Voice over IP (VoIP).

Feature History for Enhanced Voice and QoS for ADSL and G.SHDSL

Feature History	
Release	Modification
12.2(2)XQ	This feature was introduced. The Cisco 1720 did not support voice.
12.2(2)XK	Support was added for Cisco 2610-2651, Cisco 3620, Cisco 3640, and Cisco 3660.
12.2(4)XL	Support was added for Cisco 1720, Cisco 1750, Cisco 1751, and Cisco 1760.
12.2(8)YN	Enhanced voice and QoS features were added for Cisco 1720, Cisco 1721, Cisco 1751, Cisco 1760, Cisco 2610XM-2651XM, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(13)T	Enhanced voice and QoS features that were introduced in 12.2(2)XQ, 12.2(2)XK, and 12.2(4)XL were integrated into Cisco IOS Release 12.2(13)T.
12.3(2)T	Enhanced voice and QoS features that were introduced in 12.2(8)YN were integrated into Cisco IOS Release 12.3(2)T.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Enhanced Voice and QoS for ADSL and G.SHDSL

To configure the voice and QoS features, you must first install and configure the ADSL WIC or G.SHDSL WIC on your platform. Refer to the installation and configuration instructions in the following documents:

- *Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers*
- *Installing the G.SHDSL ATM WIC on the Cisco 1700 Series Router*
- 1-Port ADSL ATM WAN Interface Card for Cisco 2600 Series and 3600 Series Routers
- 1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and 3600 Series Routers
- ADSL WAN Interface Card for the Cisco 2600/3600/3700 Series
- G.SHDSL WAN Interface Card for the Cisco 2600/3600/3700 Series

For analog voice interface support, you must install the appropriate voice interface card (VIC).

Restrictions for Enhanced Voice and QoS for ADSL and G.SHDSL

- Analog and BRI voice on the NM-1V/2V cards are not supported over VoATM in AAL2.
- F5 OAM CC segment functionality is not currently supported on Cisco DSLAMs.

Information About Enhanced Voice and QoS for ADSL and G.SHDSL

The table below lists the voice and QoS feature set, the specific feature, and the release in which the features are available.

Table 16: Voice and QoS Feature Set and the Available Cisco IOS Release

Voice/QoS Feature Set	Specific Feature	Release
Classification and Marking	ATM CLP Bit Marking	12.2(8)YN
	Class-Based Packet Marking with Differentiated Services	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Committed Access Rate (CAR)	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.(8)YN, and 12.2(13)T
	Dial-Peer DSCP and IP Precedence Marking	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Local Policy Routing	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Network-Based Application Recognition (NBAR)	12.2(8)YN
	Policy-Based Routing	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
Queueing and Scheduling	Class-Based Weighted Fair Queueing (CBWFQ)	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Low Latency Queueing	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Per-VC Queueing	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
Congestion Avoidance	Class-Based WRED with DSCP (Egress)	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Resource Reservation Protocol (RSVP)	12.2(8)YN
	Weighted Random Early Detection (WRED)	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T

Voice/QoS Feature Set	Specific Feature	Release
Policing and Traffic Shaping	ATM Traffic Shaping	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Class-Based Policing	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Traffic Policing	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	VC Shaping for Variable Bit Rate-Nonreal Time (VBR-NRT)	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
Link Efficiency	cRTP over an ATM Link with PPP Encapsulation	12.2(8)YN
	Link Fragmentation and Interleaving (LFI)	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	MLP Bundling	12.2(8)YN
	PPPoE MTU Adjustment	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	Tunable Transmission Ring	12.2(8)YN
	VC Bundling	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
Other IP QoS	Access Control Lists	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
	IP QoS Map to ATM Class of Service (CoS)	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
Additional Voice/QoS	Analog Voice Interface Support	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T
Clock Rate for AAL5 and AAL2	12.2(8)YN	
Concurrent VoIP and VoATM	12.2(2)XK, 12.2(4)XL, and 12.2(8)YN	
F5 OAM CC Segment Functionality	12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
FRF.5 and FRF.8	12.2(8)YN	
H.323 and Media Gateway Control Protocol (MGCP) Testing	12.2(8)YN	
ILMI	12.2(4)XL, 12.2(8)YN, and 12.2(13)T	

Voice/QoS Feature Set	Specific Feature	Release
Multiple PVC Support	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
OAM	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
PPPoE Client	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
PPPoE over ATM	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
RFC 1483 Bridging	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
RFC 1483 Routing	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
Session Initiation Protocol (SIP)	12.2(8)YN	
Survivable Remote Site Telephony (SRST)	12.2(8)YN	
VoATM over AAL2[23]	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
VoATM over AAL51	12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	
VoIP over AAL5	12.2(2)XQ, 12.2(2)XK, 12.2(4)XL, 12.2(8)YN, and 12.2(13)T	

23 Not supported on the Cisco 1700 series.

Classification and Marking

The following Cisco IOS classification and marking features are supported on ADSL WICs and G.SHDSL WICs:

ATM CLP Bit Marking

When congestion occurs in an ATM network, ATM cells are discarded. One way to control which cells are discarded is to use the cell loss priority (CLP) bit in the ATM header of each cell. The CLP bit may be set to either 1 or 0. Those cells that have the CLP bit set to 1 are always discarded before any of the cells that have the CLP bit set to 0.

The ATM CLP Bit Marking feature allows you to control the CLP setting on Cisco routers. The marking of the CLP bit is implemented on a per-packet basis so that the CLP bit of every ATM cell that belongs to a particular packet is set to either 0 or 1.

For an example of output in which ATM CLP bit marking has been enabled, see the ATM CLP Bit Marking over G.SHDSL Example, on page 407. For more information about ATM cell bit marking, refer to When Does a Router Set the CLP Bit in an ATM Cell

Class-Based Packet Marking with Differentiated Services

For information about class-based packet marking with differentiated services, refer to the "Quality of Service Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Committed Access Rate

For information about committed access rate (CAR), refer to the "Quality of Service Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Dial-Peer DSCP and IP Precedence Marking

For information about dial-peer differentiated services code points (DSCPs) and IP precedence marking, refer to the "Quality of Service for Voice over IP" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Local Policy Routing

For information about local policy routing (LPR), refer to the following documents:

- "Configuring IP Routing Protocol--Independent Features" chapter in the Cisco IOS IP Configuration Guide
- "Configuring IP Routing Protocols" chapter in the Router Products Configuration Guide

Network-Based Application Recognition

For information about network-based application recognition (NBAR), refer to the following documents:

- Network-Based Application Recognition
- Using Content Networking to Provide Quality of Service
- "Configuring Network-Based Application Recognition" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*

Policy-Based Routing

For information about policy-based routing (PBR), refer to the following documents:

- "Quality of Service Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*

Queueing and Scheduling

The following Cisco IOS queueing and scheduling features are supported on ADSL WICs and G.SHDSL WICs:

Class-Based Weighted Fair Queueing

For information about class-based weighted fair queueing (CBWFQ), refer to "Quality of Service Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Low Latency Queueing

For information about low latency queueing (LLQ), refer to the following documents:

- "Congestion Management Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Low latency queueing works in conjunction with setting the transmission (tx) ring. For more information about setting the tx ring, see the Tunable Transmission Ring, on page 358.

Per-VC Queueing

Per-virtual circuit (per-VC) queueing is supported on ADSL and G.SHDSL interfaces at the driver level, similar to VC-queueing features on other ATM interfaces. This feature underlies many of the Cisco IOS QoS queueing features, such as LLQ.

For more information about per-VC queueing, refer to the following documents:

- *Understanding Weighted Fair Queuing on ATM*
- *Per-VC Class-Based, Weighted Fair Queuing (Per-VC CBWFQ) on the Cisco 7200, 3600, and 2600 Routers*

Congestion Avoidance

The following Cisco IOS congestion avoidance features are supported on ADSL WICs and G.SHDSL WICs:

Class-Based Weighted Random Early Detection with DSCP at Egress

Class-Based Weighted Random Early Detection (WRED) is supported on ADSL and G.SHDSL WICs. For more information about WRED, refer to the following documents:

- "Quality of Service Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*
- *Cisco IOS Quality of Service Solutions Command Reference*

- *DiffServ Compliant Weighted Random Early Detection*

Resource Reservation Protocol

For information about Resource Reservation Protocol (RSVP), refer to the following documents:

- "Configuring RSVP" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*
- "Configuring RSVP Support for LLQ" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*
- "Configuring RSVP Support for Frame Relay" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*
- "Configuring RSVP-ATM QoS Interworking" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*

Weighted Random Early Detection

For information about Weighted Random Early Detection (WRED), refer to the "Configuring Weighted Random Early Detection" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Policing and Traffic Shaping

The following Cisco IOS policing and shaping features are supported on ADSL WICs and G.SHDSL WICs:

ATM Traffic Shaping

For information about ATM traffic shaping, refer to the following document:

- Configuring Traffic Shaping on Frame Relay to ATM Service Interworking (FRF.8) PVCs
- "Policing and Shaping Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*

Class-Based Policing

For information about traffic classes and traffic policies, refer to the "Configuring Traffic Policing" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Traffic Policing

For information about traffic policing, refer to the following documents:

- "Configuring Traffic Policing" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*
- *Comparing Class-Based Policing and Committed Access Rate*

VC Shaping for Variable Bit Rate-Nonreal Time

For information about VC shaping for variable bit rate-nonreal time (VBR-NRT), refer to *Understanding the VBR-nrt Service Category and Traffic Shaping for ATM VCs* .

Link Efficiency

The following link latency features are supported on ADSL WICs and G.SHDSL WICs:

cRTP over an ATM Link with PPP Encapsulation

The Compressed Real-Time Protocol (cRTP) feature reduces bandwidth consumption on real-time applications such as voice. Thus, by using cRTP, you can further improve voice quality. Configuring cRTP can save troubleshooting time by isolating potential cRTP issues. Based on RFC 2508, the RTP header compression feature compresses the IP, User Data Protocol (UDP), and Real-Time Transport Protocol (RTP) header (IP/UDP/RTP header) from 40 bytes to 2 or 4 bytes, reducing unnecessary bandwidth consumption. RTP header compression is a hop-by-hop compression scheme; therefore, cRTP must be configured on both ends of the link (unless the passive option is configured).

To configure cRTP, use the **ip rtp header-compression** command.

Because the compression process can be CPU intensive, RTP header compression was implemented in the fast-switching and Cisco Express Forwarding (CEF) switching paths in Cisco IOS Release 12.0(7)T. Sometimes the cRTP implementations are broken, and if they are broken, the only way that cRTP will work is to use process switching. It is recommended that cRTP be used with links lower than 768 kbps unless the router is running at a low CPU utilization rate. Monitor the CPU utilization of the router, and disable cRTP if it is above 75 percent.

When you configure the **ip rtp header-compression** command, the router adds the **ip tcp header-compression** command to the configuration by default. The **ip tcp header-compression** command is used to compress the TCP/IP packets of the headers. Header compression is particularly useful on networks that have a large percentage of small packets, such as those supporting many Telnet connections. The TCP header compression technique, described fully in RFC 1144, is supported on serial lines that use High-Level Data Link Control (HDLC) or PPP encapsulation.

To compress the TCP headers without enabling cRTP, use the **ip tcp header-compression**command.

To enable the cRTP over an ATM Link with PPP Encapsulation feature, see the Configuring cRTP over an ATM Link with ATM Encapsulation, on page 372.

Link Fragmentation and Interleaving

For information about the Link Fragmentation and Interleaving (LFI) feature, refer to the "Configuring Link Fragmentation and Interleaving for Frame Relay and ATM Virtual Circuits" chapter in the Cisco IOS Quality of Service Solutions Configuration Guide.

MLP Bundling

Multilink PPP (MLP), standardized in RFC 1990, is similar to load-balancing techniques in that it sends packets across the individual links in a round-robin fashion. However, MLP adds three significant capabilities:

- Because MLP works at the link layer, it makes an MLP bundle appear as one logical link to the upper layer protocols in the router. Thus, only one network address needs to be configured for the entire MLP bundle.
- MLP keeps track of packet sequencing and buffers packets that arrive early. With this ability, MLP preserves packet order across the entire MLP bundle.
- Packet fragmentation can be enabled to split large data packets into smaller packet fragments that are individually transmitted across the links. In many circumstances, fragmentation can increase the efficiency of the MLP link.

Additionally, when more bandwidth is needed, additional links can be added to the bundle by simply configuring them as members of the bundle. No reconfiguration at the network layer, such as new addressing, is needed. This is also a significant factor when considering the use of advanced router services. For example, a specific QoS can be configured once for the bundle as a whole rather than on each link in the bundle.

The trade-off for the increased functionality is that MLP requires greater CPU processing than load-balancing solutions. Packet reordering, fragment reassembly, and the MLP protocol itself increase the CPU load.

Note The fragment delay on the multilink interface should be configured on the basis of the desired maximum delay for interleaved packets. Interleaving is useful only at low bandwidths, usually below 1 Mbps, and it is dependent on the link bandwidths, not the bundle bandwidth.

- It is recommended that IP CEF be turned on. IP CEF will result in better performance and ease of configuration.
- The virtual template (VT) should be used (instead of the dialer interface) when configuring either authentication or dynamic address assignment for MLP with LFI.

To enable MLP bundling, see the section "Configuring MLP Bundling, on page 395."

PPPoEMTUAdjustment

If a Cisco router terminates the PPP over Ethernet (PPPoE) traffic, a computer connected to the Ethernet interface may have a problem accessing websites. The solution is to manually reduce the maximum transmission unit (MTU) configured on the computer by constraining the TCP maximum segment size (MSS). To manually reduce the MTU configured on the computer, use the **ip tcp adjust-mss**command. The *mss* argument value must be 1452 or less.

For more information about adjusting the PPPoE MTU, refer to *Software Enhancements for the Cisco 800 Routers and SOHO Routers.*

Tunable Transmission Ring

The transmission (tx) ring is the FIFO buffer used to hold frames before transmission at the DSL driver level. The tx ring defines the maximum number of packets that can wait for transmission at Layer 2.

The tx ring complements the ability of LLQ to minimize jitter and latency of voice packets. For maximum voice quality, a low tx ring setting should be used. For maximum data throughput, a high tx ring setting should be used.

You can configure the size of the tx ring for each permanent virtual circuit (PVC). The default value is 60. However, the value of the setting can be 1 through 60 on Cisco 1700 series routers and 3 through 60 on Cisco 2600 and Cisco 3600 series routers. A low tx ring setting, such as 2 or 3, is required for latency-critical traffic. For example, when the tx ring limit is configured as 3 and LLQ is configured on the PVC, the worst case delay for a voice packet is the time required to transmit three data packets. When the buffering is reduced by configuring the tx ring limit, the delay experienced by voice packets is reduced by a combination of the tx ring and LLQ mechanism.

Note The size of the tx ring buffer is measured in packets, not particles.

VC Bundling

For information about virtual circuit (VC) bundling, refer to *Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers* .

Other IP QoS

The following IP QoS features are supported on ADSL WICs and G.SHDSL WICs:

Access Control Lists

For information about access control lists, refer to the "Configuring IP Services" chapter in the *Cisco IOS IP Configuration Guide*.

IP QoS Map to ATM Class of Service

For information about IP QoS map to ATM class of service (CoS), refer to the "Configuring IP to ATM Class of Service" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Additional Supported Features

The following Cisco IOS features are supported on ADSL WICs and G.SHDSL WICs:

Analog Voice Interface Support

Note The Analog Voice Interface Support feature requires an appropriate VIC.

For more information about analog voice interface support, refer to the Voice Port Testing Enhancements in Cisco 2600 and 3600 Series Routers and MC3810 Series Concentrators.

Clock Rate for AAL5 and AAL2

The communication between DSL WICs and a host in a router occurs through a device called the Serial Communication Controller (SCC). If a host wants to forward data or send any control traffic to a DSL WIC, it uses SCCs. In the same way, if a DSL WIC wants to forward incoming data from a line to the host, it also uses SCCs. Each DSL WIC installed in the router uses two SCCs. One SCC (SCC-A) is used for ATM adaptation layer 5 (AAL5) data traffic, and the other SCC (SCC-B) is used for ATM adaptation layer 2 (AAL2) and control traffic. The speed at which the SCC transfers data between a host and a WIC depends on the clock rate with which it has been configured. You can configure this clock rate on the basis of the DSL line rate. Even though the DSL upstream and downstream line rate may vary, the clock rate between the SCC and the DSL WIC is the same for both the transmitting and receiving direction. That is, the communication between the SCC and the DSL WIC is synchronous. Therefore, you need to configure only one clock rate for an SCC that will be used for both transmitting and receiving between an SCC and a DSL WIC.

It is always recommended that you configure the SCC clock rate slightly higher than the DSL line rate to accommodate overhead between the SCC and the DSL WIC. For an asynchronous DSL WIC (for example, ADSL), the SCC clock rate depends on either the downstream or the upstream line rate, whichever is the maximum rate. For a synchronous DSL WIC (for example, G.SHDSL), the bandwidth for upstream and downstream is the same. Therefore, the SCC clock rate configuration can be based on either the upstream or the downstream line rate.

To configure the clock, use the **clock rate** command, which is shown in the Configuring the Clock Rate for ADSL and G.SHDSL WICs, on page 367.

Maximum Clock Rate Limits and Defaults

Because the maximum line rate for G.SHDSL is 2.312 Mbps, the default SCC clock rate of 2.6 Mbps for AAL5 and 1 Mbps for AAL2 should be sufficient. However, for ADSL, the clock rate may need to be configured on the basis of the current line rate. If AAL2 is used for voice traffic, the AAL2 SCC must be configured to the appropriate clock rate: 1 Mbps for ADSL and 2.6 Mbps for G.SHDSL.

The maximum data rate between an SCC and a DSL WIC depends primarily on the maximum clock rate that the SCC can support. For example, on the Cisco 2600 series mainboard, which supports two DSL WICs, the total SCC clock rate that can be configured for both WICs is 8 Mbps. Therefore, if only one DSL WIC is present on the mainboard, AAL5 and AAL2 clock rates can be configured to 7 Mbps and 1 Mbps, respectively. If two DSL WICs are supported on the mainboard, the total of 8 Mbps should be distributed among the four SCCs.

Network module SCCs also pose similar limitations. That is, on the Cisco 2600 series, the total clock rate for all four SCCs is 8 Mbps. The maximum AAL5 clock rate that may be configured on a network module is 5.3 Mbps. On the Cisco 1700 series, the maximum configurable SCC clock rate for both AAL5 and AAL2 is 8 Mbps.

If the clock rate is unconfigured, the SCC is reset to the default values. See the **clock rate** (interface ATM) command for a complete explanation of default values and maximum and minimum values.

Concurrent VoIP and VoATM

The Concurrent VoIP and VoATM feature allows you to make VoIP over ATM (aal5snap) and VoATM (aal5mux) calls concurrently over xDSL.

Note This feature is not supported on the Cisco 1700 series.

F5 OAM CC Segment Functionality

For information about F5 Operation, Administration, and Maintenance Continuity Check (F5 OAM CC) segment functionality, refer to the following documents:

- *Cisco Product Bulletin No. 1518 about Cisco IOS Release 12.2(2)XJ*
- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(2)XJ*

FRF.5 and FRF.8

To communicate over WANs, end-user stations and the network cloud typically must use the same type of transmission protocol. This limitation has prevented differing networks such as Frame Relay and ATM from being linked. The Frame Relay-to-ATM service interworking feature allows Frame Relay and ATM networks to exchange data despite differing network protocols. The functional requirements for linking Frame Relay and ATM networks are provided by the *Frame Relay/ATM PVC Service Interworking Implementation Agreement* specified in Frame Relay Forum (FRF) documents FRF.5 and FRF.8. The FRF.5 and FRF.8 interworking functions involve multiplexing PVCs between Frame Relay and ATM networks and mapping the control bits between Frame Relay frame headers and ATM cell headers. FRF.5 and FRF.8 are necessary for ATM-based features to interwork with Frame-Relay-based IP class of service features.

To configure FRF.5 and FRF.8, see Configuring FRF.5 One-To-One Connections, on page 381 and Configuring FRF.8, on page 390.

H.323 and Media Gateway Control Protocol

For information about H.323 and Media Gateway Control Protocol (MGCP) testing, refer to *Cisco IOS H.323 Configuration Guide* in the *Cisco IOS Voice Configuration Library*.

ILMI

For information about Integrated Local Management Interface (ILMI) protocol implementation for Cisco digital subscriber loop access multiplexers (DSLAMs) with N1-2 cards, refer to the "Configuring ILMI" chapter in the *Configuration Guide for Cisco DSLAMS with N1-2* .

Multiple PVC Support

Note The maximum number of PVCs that can be supported is 23.

For information about PVCs, refer to the following documents:

- "Wide-Area Networking Overview" chapter in *Cisco IOS Wide-Area Networking Configuration Guide*

- "Configuring ATM" chapter in the *Cisco IOS Asynchronous Transfer Mode Configuration Guide*

Refer to the following documents for caveat information for multiple PVCs by platform for Cisco IOS Release 12.2(2)XK:

- Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(2)XK
- Release Notes for Cisco 2600 Series for Cisco IOS Release 12.2 XK
- Release Notes for Cisco 3600 Series for Cisco IOS Release 12.2 XK

Refer to the following documents for caveat information for multiple PVCs by platform for Cisco IOS Release 12.2(4)XL:

- Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(4)XL
- Release Notes for Cisco 2600 Series for Cisco IOS Release 12.2 XL
- Release Notes for Cisco 3600 Series for Cisco IOS Release 12.2 XL

Refer to the *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(8)YN* document for caveat information for multiple PVCs.

OAM

For information about Operation, Administration, and Maintenance (OAM), refer to the *Configuring Operation, Administration, and Maintenance* document.

PPPoE Client

For information about the Point-to-Point Protocol over Ethernet (PPPoE) Client feature, refer to the *PPP over Ethernet Client* document.

PPPoE over ATM

PPPoE over ATM enables PPP sessions to be transported using an Ethernet-connected PC over an ATM DSL link. For more information about the PPPoE over ATM feature, refer to the *PPPoE on ATM* document.

RFC 1483 Bridging

For information about RFC 1483 bridging, refer to the following documents:

- *Basic PVC Configuration Using Bridged RFC 1483*
- DSL Network Architectures

RFC 1483 Routing

For information about ATM and ATM adaptation layers (AALs), refer to the "Wide-Area Networking Overview" chapter in *Cisco IOS Wide-Area Networking Configuration Guide*.

Session Initiation Protocol

For information about Session Initiation Protocol (SIP), refer to *Cisco IOS SIP Configuration Guide* in the Cisco IOS Voice Configuration Library .

Survivable Remote Site Telephony

For information about Survivable Remote Site Telephony (SRST), refer to the *Survivable Remote Site Telephony Cisco 2600/3600 Voice Technical Marketing* solutions document.

VoATM over AAL2

For information about Voice over ATM over AAL2, refer to the following documents:

- "Configuring Voice over ATM" chapter in the Cisco IOS Voice Configuration Library
- Configuring AAL2 and AAL5 for the High-Performance ATM Advanced Integration Module on the Cisco 2600 Series

Note The Voice over ATM over AAL2 feature is not supported on the Cisco 1700 series.

VoATM over AAL5

For information about Voice over ATM over AAL5, refer to the Cisco IOS Voice Configuration Library .

Note This feature is not supported on the Cisco 1700 series.

VoIP over AAL5

For information about Voice over IP over AAL5, refer to the Cisco IOS Voice Configuration Library .

Benefits of QoS

QoS provides improved and more predictable network service for ADSL and G.SHDSL by

- Supporting dedicated bandwidth.
- Improving loss characteristics.
- Avoiding and managing network congestion.
- Shaping network traffic.
- Setting traffic priorities across the network.

- Decreasing delay for voice and real-time traffic.

How to Configure Enhanced Voice and QoS for ADSL and G.SHDSL

Configuring ATM CLP Bit Marking

This task shows you how to configure ATM CLP bit marking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **class-map** *class-map-name*
5. **match access-group** *access-group*
6. **exit**
7. **policy-map** *policy-map-name*
8. **class** *name*
9. **set atm-clp**
10. **exit**
11. **exit**
12. **interface** *type slot* / *port* . *subinterface-number* [**multipoint** | **point-to-point**]
13. **pvc** *vpi* / *vci*
14. **service-policy output** *policy-map-name*

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.

	Command or Action	Purpose
Step 3	**ip cef** **Example:** `Router(config)# ip cef`	Enables Cisco Express Forwarding (CEF).
Step 4	**class-map** *class-map-name* **Example:** `Router(config)# class-map abc`	Creates a class map to be used for matching packets to a specified class and enters class map configuration mode. The *class-map-name* argument is the name of the class for the class map. The class name is used for both the class map and to configure policy for the class in the policy map.
Step 5	**match access-group** *access-group* **Example:** `Router(config-cmap)# match access-group 199`	Specifies the numbered access list against whose contents packets are checked to determine whether they belong to the class. Refer to the Cisco IOS Quality of Service Solutions Configuration Guide for other **match** options.
Step 6	**exit** **Example:** `Router(config-cmap)# exit`	Exits class map configuration mode.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map anyrule`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy map configuration mode. The *policy-map-name* argument is the name of the policy map.
Step 8	**class** *name* **Example:** `Router(config-pmap)# class abc`	Specifies the name of a traffic class to classify traffic for the policy traffic and enters policy-map class configuration mode. The *name* argument should be the same as the class-map name in Step 4 of this configuration.
Step 9	**set atm-clp** **Example:** `Router(config-pmap-c)# set atm-clp`	Controls the cell loss priority (CLP) bit setting on Cisco routers when a policy map is configured (changes the setting for all packets that match the specified class from 0 to 1).
Step 10	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 12	**interface** *type slot* / *port* . *subinterface-number* [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/1.299 multipoint`	Configures an interface type and enters subinterface configuration mode. The arguments and keywords are as follows: • *type* --To configure ATM CLP bit marking, use atm for the *type* argument. • *slot* --Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information. • *port* --Number of the port being configured. Refer to the appropriate hardware manual for slot and port information. • *subinterface-number* --Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs. • **multipoint--** (Optional) Multipoint subinterface. • *point-to-point* --(Optional) Point-to-point subinterface.
Step 13	**pvc** *vpi* / *vci* **Example:** `Router(config-subif)# pvc 1/1`	Creates an ATM permanent virtual circuit (PVC) or assigns a name to an ATM PVC and enters ATM VC configuration mode. The arguments are as follows: • *vpi* / --ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a VPI value defaults the VPI value to 0. • *vci* --ATM network virtual channel identifier (VCI) for this PVC. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. **Note** The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
Step 14	**service-policy output** *policy-map-name* **Example:** `Router(config-if-atm-vc)# service-policy output abc`	Attaches a policy map to an interface to be used as the service policy for that interface. The arguments and keywords are as follows: • **output** --Attaches the specified policy map to the output interface. • *policy-map-name* --Name of a service policy map (created using the **policy-map** command) to be attached.

Verifying ATM CLP Bit Marking

The following is sample output using the **show atm pvc** command on a Cisco 1721 router that show detailed information about the PVC. In this example, five packets are sent, with the CLP set to 1.

```
Router# show atm pvc 0/33
ATM0.1: VCf: 1, VPI: 0, VCI: 33
UBR, PeakRate: 2304
AAL5-LLC/SNAP, etype:0x0, Flags: 0x2000C20, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM END CC Activate retry count: 3, OAM END CC Deactivate retry count: 3
OAM END CC retry frequency: 30 second(s),
OAM SEGMENT CC Activate retry count: 3, OAM SEGMENT CC Deactivate retry count: 3
OAM SEGMENT CC retry frequency: 30 second(s),
OAM Loopback status: OAM Disabled
OAM VC state: Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minutes(s)
InPkts: 5, OutPkts: 5, InBytes: 560, OutBytes: 560
InPRoc: 5, OutPRoc: 5
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0/0/0 (holdq/outputq/total)
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 5
OAM cells receivef: 0
F5 InEndloop: 0, F5 InSegloop: 0,
F5 InEndcc: 0, F5 InSegcc: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0,
F5 OutEndcc: 0, F5 OutSegcc: 0, F5 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

Configuring the Clock Rate for ADSL and G.SHDSL WICs

To configure the clock between a WIC and the hosts that are used by the WIC, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *port*
4. **clock rate** [**aal2**| **aal5**] *clock-rate-value*
5.
6.
7.
8.
9. **no clock rate aal5** | **aal2**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *port* **Example:** `Router(config)# interface atm 0/1`	Configures an ATM interface type and enters interface configuration mode.
Step 4	**clock rate** [**aal2**| **aal5**] *clock-rate-value* **Example:** `Router(config-if)# clock rate aal2 4000000`	Configures the clock rate between a WIC and the SCCs that are used by the WIC. The keywords and arguments are as follows: • **aal2** --Clock rate for the AAL2 channel. • **aal5** --Clock rate for the AAL5 channel.
Step 5		• *clock-rate-value* --The clock rate can be set as follows: • **aal2**--For Cisco 1700 series routers, the minimum value for ADSL and G.SHDSL is 4 Mbps. The default value for ADSL and G.SHDSL is 8 Mbps. For Cisco 2600 and 3600 series routers, the minimum value for ADSL and G.SHDSL is 1 Mbps. The maximum value is 7 Mbps for mainboard slots and 5.3 Mbps for network modules. The default value for ADSL and G.SHDSL is 2.6 Mbps for both mainboard slots and network modules. To make full use of the 2.3 Mbps bandwidth for VoATM non-switched trunk calls on G.SHDSL, you can change the 1 Mbps default value on Cisco 2600 series and Cisco 3600 series routers and configure the AAL2 clock rate as 2.6 Mbps.
Step 6		It is recommended, however, that you keep the ADSL SCC clock rate for AAL2 at the default value of 1 Mbps because the upstream of ADSL cannot exceed 1 Mbps.
Step 7		**Note** Change the AAL2 default value on Cisco 2600 and Cisco 3600 series routers only if you are using G.SHDSL for VoATM non-switched trunk calls using a NM-HDV. All other times, the default for AAL2 should remain at 1 Mbps for ADSL and G.SHDSL.
Step 8		• • **aal5** --For Cisco 1700 series routers, the minimum value for ADSL and G.SHDSL is 4 Mbps. The default value for ADSL and G.SHDSL is 8 Mbps.

	Command or Action	Purpose
		For Cisco 2600 and 3600 series routers, the minimum value for ADSL and G.SHDSL is 1 Mbps. The maximum value is 7 Mbps for mainboard slots and 5.3 Mbps for network modules. The default value for ADSL and G.SHDSL is 2.6 Mbps for both mainboard slots and network modules. **Note** If you configure a clock rate that exceeds the maximum limit, the configuration will fail. (See the section Troubleshooting the Clock Setting for ADSL and G.SHDSL WICs, on page 371.)
Step 9	**no clock rate aal5 | aal2** **Example:** `Router(config-if)# no clock rate aal5`	Disables the clock setting for AAL5 or AAL2, respectively, and changes the clock rate to the default setting. The other method for changing the AAL5 or AAL2 clock rate into the default rate is to configure the clock rate to the actual default settings.

Verifying the Clock Setting for ADSL and G.SHDSL WICs

To verify the clock rate setting for an ADSL WIC or G.SHDSL WIC on a Cisco 1700, Cisco 2600, or Cisco 3600 series router, use the **show running-config** or the **show controllers atm**command in EXEC mode.

Cisco 1700 Series Router

```
Router# show running-config interface atm0/0
interface ATM0/0
 ip address 1.0.0.1 255.255.255.0
 no ip route-cache
 load-interval 30
 clock rate aal2 4000000
 no atm ilmi-keepalive
 pvc 0/33
!
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
```

Cisco 1700 Series Router

```
Router# show controllers atm0/0
Interface: ATM0/0, Hardware: DSLSAR (with Globespan G.SHDSL module), State:
up
IDB:     82201E98 Instance: 8220364C reg_dslsar:68030000 wic_regs:
68030080
PHY Inst:822251DC Ser0Inst: 821FC328 Ser1Inst: 821FF41C us_bwidth:192
Slot:     0         Unit:     0          Subunit:    0         pkt Size: 4528
VCperVP: 256        max_vp:   256        max_vc:     65536     total vc: 1
rct_size:65536      vpivcibit:16         connTblVCI:8          vpi_bits: 8
vpvc_sel:3          enablef:  0          throttlef: 0          cell drops:
0
Parallel reads to TCQ:0  tx count reset = 0, periodic safe start = 0
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 9, current queue depth = 0, drops = 0, urun
cnt = 0,
```

```
total cnt = 153
Serial idb tx count: AAL5: 0, RAW: 0, Drop count:AAL5: 0, RAW: 0
SCC Clockrates:
    SCC-A = 8000000
    SCC-B = 4000000
```

In the above example, SCC-A represents the SCC clock rate for AAL5 and SCC-B represents the SCC clock rate for AAL2.

Cisco 2600 Series Chassis WIC Slots

The following **show controllers atm** example from a Cisco 2621 router shows verification of the SCC clock rates for ATM interface 0/0 on mainboard slot 0 and ATM interface 0/1 on mainboard slot 1:

```
Router# show controllers atm 0/0
Interface: ATM0/0, Hardware: DSLSAR (with Globespan G.SHDSL module), State: up
IDB:     8295D918  Instance: 8295F0CC  reg_dslsar:67000000  wic_regs: 67000080
PHY Inst:82981024  Ser0Inst: 8294C2B4  Ser1Inst:  82954DD8  us_bwidth:2304
Slot:    0         Unit:     0         Subunit:   0         pkt Size: 4528
VCperVP: 256       max_vp:   256       max_vc:    65536     total vc: 2
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits: 8
vpvc_sel:3         enablef:  0         throttlef: 0         cell drops: 0
Parallel reads to TCQ:2  tx count reset = 0, periodic safe start = 0
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 10, current queue depth = 0, drops = 0, urun cnt = 0, total cnt
 = 105
Serial idb tx count: AAL5: 90277249, RAW: 105, Drop count:AAL5: 0, RAW: 0
SCC Clockrates:
        SCC0 = 2600000 (ATM0/0)
        SCC1 = 2600000 (ATM0/1)
        SCC2 = 1000000 (ATM0/1)
        SCC3 = 1000000 (ATM0/0)
```

In the above example, the ADSL WIC in slot 0 uses SCC0 and SCC3. The AAL5 and AAL2 SCC clock rate of the WICs are 2 Mbps and 4 Mbps, respectively. The second WIC in slot 1 uses SCC1 and SCC2 for AAL5 and AAL2.

Cisco 2600 Series Network Router

The SCC assignment on a network module is different. The following **show controllers atm** example is from ATM interface 1/0, which is on network module slot 0. The example is from a Cisco 2650XM router.

```
Router# show controllers atm1/0
Interface: ATM0/0, Hardware: DSLSAR (with Globespan G.SHDSL module), State: up
IDB:     8295D918  Instance: 8295F0CC  reg_dslsar:67000000  wic_regs: 67000080
PHY Inst:82981024  Ser0Inst: 8294C2B4  Ser1Inst:  82954DD8  us_bwidth:2304
Slot:    0         Unit:     0         Subunit:   0         pkt Size: 4528
VCperVP: 256       max_vp:   256       max_vc:    65536     total vc: 2
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits: 8
vpvc_sel:3         enablef:  0         throttlef: 0         cell drops: 0
Parallel reads to TCQ:2  tx count reset = 0, periodic safe start = 0
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 10, current queue depth = 0, drops = 0, urun cnt = 0, total cnt
 = 105
Serial idb tx count: AAL5: 90277249, RAW: 105, Drop count:AAL5: 0, RAW: 0
SCC Clockrates:
        SCC0 = 2600000 (ATM0/0)
        SCC1 = 2600000 (ATM0/1)
        SCC2 = 1000000 (ATM0/1)
        SCC3 = 1000000 (ATM0/0)
```

Troubleshooting the Clock Setting for ADSL and G.SHDSL WICs

The system limitation for Cisco 2600 and Cisco 3600 series routers is that the total SCC clock rate that can be configured for one or more WICs is 8 Mbps. The following troubleshooting tips for Cisco 2600 and Cisco 3600 routers explain situations for which warning and error messages can be received because of the 8 Mbps limitation.

SUMMARY STEPS

1. If you configure a clock rate that exceeds the maximum limit, the configuration will fail. In the following example (on a Cisco 2621 router), both the AAL5 SCC and the AAL2 SCC have been configured to 4 Mbps. Then an additional 7 Mbps are configured on the AAL5 SCC.
2. If you have already configured your DSL WIC and then add a second WIC, you may exceed the maximum Mbps limit and receive a message such as the following, which shows that the failed DSL interface is shut down and that the clock rates are set to zero:
3. Non-DSL WICs, such as serial WICs, do not restrict you from configuring more than the maximum SCC clock rate. If these non-DSL WICs coexist with DSL WICs, the dynamic SCC clock rate configuration for the non-DSL WIC is monitored and checked for the maximum limit. If the total SCC clock rate exceeds the maximum limit, the %DSLSAR-1-NO_SCC_CLK_ERR message is displayed and DSL interfaces are shut down. In this case, the SCC clock rates of the shut-down DSL interface are not reset to zero. If you reconfigure the SCC clock rate so that the current clock rate is less than or equal to the maximum limit, the shut-down interface is automatically brought up and the error message will cease to display.

DETAILED STEPS

Step 1 If you configure a clock rate that exceeds the maximum limit, the configuration will fail. In the following example (on a Cisco 2621 router), both the AAL5 SCC and the AAL2 SCC have been configured to 4 Mbps. Then an additional 7 Mbps are configured on the AAL5 SCC.
The following error message indicates that the maximum clock rate configured on the AAL5 SCC is 4 Mbps, including the existing clock rate:

Example:

```
Router (config)# interface atm 0/0
Router (config-if)# clock rate aal5 7000000
%error: insufficient clockrates, available (including current clock rate) = 4000000 bps
%Clockrate configuration failed
```

Step 2 If you have already configured your DSL WIC and then add a second WIC, you may exceed the maximum Mbps limit and receive a message such as the following, which shows that the failed DSL interface is shut down and that the clock rates are set to zero:

Example:

```
1d20h: %DSLSAR-1-NO_SCC_CLK_ERR: ATM1/0: Interface is DOWN because the sum of the clock rate values
 for both the WICs in slots 0 and 1 exceeded maximum capacity. Please configure clock rates using
clock rate command in interface mode such that the sum of clock rate on both the WICs does not exceed
 8000000 bps. For a DSL wic, please include aal5 and aal2 clock rate values while calculating the
total.
```

If you add a second WIC, make sure that you reduce the clock rate of the existing DSL so that the combined clock rates do not exceed the maximum.

Step 3 Non-DSL WICs, such as serial WICs, do not restrict you from configuring more than the maximum SCC clock rate. If these non-DSL WICs coexist with DSL WICs, the dynamic SCC clock rate configuration for the non-DSL WIC is monitored and checked for the maximum limit. If the total SCC clock rate exceeds the maximum limit, the %DSLSAR-1-NO_SCC_CLK_ERR message is displayed and DSL interfaces are shut down. In this case, the SCC clock rates of the shut-down DSL interface are not reset to zero. If you reconfigure the SCC clock rate so that the current clock rate is less than or equal to the maximum limit, the shut-down interface is automatically brought up and the error message will cease to display.

Configuring cRTP over an ATM Link with ATM Encapsulation

This task shows you how to configure cRTP over an ATM link with ATM encapsulation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **class-map** [**match-all]** *class-map-name*
5. **match access-group name** *access-group-number*
6. **class-map** [**match-all**] *class-map-name*
7. **match access-group name** *access-group-number*
8. **policy-map** *policy-map-name*
9. **class** *class-name*
10. **priority** {*bandwidth-kbps* | **percent***percentage*}
11. **fair-queue** [**queue-limit** *queue-value*]
12. **exit**
13. **exit**
14. **interface** *type interface-number*
15. **ip address** *ip-address mask* [**secondary**]
16. **interface atm** *slot* / *port*
17. **no ip address**
18. **load-interval** *seconds*
19. **no atm ilmi-keepalive**
20. **pvc** *vpi* / *vci*
21. **vbr-rt** *peak-rate average-rate burst*
22. **tx-ring-limit** *ring-limit*
23. **protocol** *protocol* {**virtual-template** {*virtual-template-interface-number*}| **dialer**}
24. **exit**
25. **dsl equipment-type** {**co** | **cpe**}
26. **dsl operating-mode auto gshdsl symmetric annex** {**A** | **B**}
27. **dsl linerate** {*kbps* | **auto**}
28. **exit**
29. **interface virtual-template** *number*
30. **ip unnumbered** *type-number*
31. **ip tcp header-compression**
32. **service-policy** {**input** | **output**}
33. **ppp multilink**
34. **ppp multilink fragment-delay** *delay-max*
35. **ppp multilink interleave**
36. **ip rtp header-compression** [**passive**]
37. **ip rtp compression-connections** *number*
38. **exit**
39. **voice-port** *slot-number* / *subunit-number* / *port*

40. **dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**}
41. **destination-pattern** [+] *string* [**T**]
42. **port** {*slot-number* / *subunit-number* / *port*}
43. **exit**
44. **dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**}
45. **destination-pattern** [+] *string* [**T**]
46. **session target** {**ipv4:** *destination-address*}
47. **dtmf-relay** [**cisco-rtp**] [**h245-alphanumeric**] [**h245-signal**]
48. **ip qos dscp** [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**]
49. **ip qos dscp** [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**]
50. **no vad**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** **Example:** `Router(config)# ip cef`	Enables Cisco Express Forwarding (CEF) on the Route Processor card.
Step 4	**class-map** [**match-all**] *class-map-name* **Example:** `Router(config)# class-map match-all voice-traffic`	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode.
Step 5	**match access-group name** *access-group-number* **Example:** `Router(config-cmap)# match access-group 102`	Configures the match criteria for a class map on the basis of the specified access control list (ACL).

	Command or Action	Purpose
Step 6	**class-map** [**match-all**] *class-map-name* **Example:** `Router(config-cmap)# class-map match-all voice-signaling`	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode.
Step 7	**match access-group name** *access-group-number* **Example:** `Router(config-cmap)# match access-group 103`	Configures the match criteria for a class map on the basis of the specified ACL.
Step 8	**policy-map** *policy-map-name* **Example:** `Router(config-cmap)# policy-map VOICE-POLICY`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy-map configuration mode.
Step 9	**class** *class-name* **Example:** `Router(config-pmap)# class voice-traffic`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
Step 10	**priority** {*bandwidth-kbps* | **percent***percentage*} **Example:** `Router(config-pmap)# priority 8 48`	Gives priority to a class of traffic belonging to a policy map.
Step 11	**fair-queue** [**queue-limit** *queue-value*] **Example:** `Router(config-pmap)# fair-queue`	Specifies the number of queues to be reserved for use by a traffic class.
Step 12	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 13	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode.

	Command or Action	Purpose
Step 14	**interface** *type interface-number* **Example:** `Router(config)# interface loopback1`	Enters interface configuration mode. Use Loopback for the *type*argument. Use 1 for the *interface-number* argument. Loopback 1 is a standard configuration for Multilink PPP (MLP) over ATM.
Step 15	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 172.100.10.10 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 16	**interface atm** *slot* / *port* **Example:** `Router(config-if)# interface atm 0/1`	Configures an ATM interface type.
Step 17	**no ip address** **Example:** `Router(config-if-atm)# no ip address`	Removes an IP address or disables IP processing.
Step 18	**load-interval** *seconds* **Example:** `Router(config-if-atm)# load-interval 15`	Changes the length of time for which data is used to compute load statistics.
Step 19	**no atm ilmi-keepalive** **Example:** `Router(config-if-atm)# no atm ilmi-keepalive`	Disables ILMI keepalive.
Step 20	**pvc** *vpi* / *vci* **Example:** `Router(config-if-atm)# pvc 1/100`	Creates an ATM permanent virtual circuit (PVC) or assigns a name to an ATM PVC and enters ATM VC configuration mode.
Step 21	**vbr-rt** *peak-rate average-rate burst* **Example:** `Router(config-if-atm-vc)# vbr-rt 1500 1500`	Configures the real-time variable bit rate (VBR) for Voice over ATM connections.

	Command or Action	Purpose
Step 22	**tx-ring-limit** *ring-limit* **Example:** `Router(config-if-atm-vc)# tx-ring-limit 3`	Limits the number of particles or packets that can be used on a transmission ring on an interface. The *ring-limit* argument specifies the maximum number of allowable particles or packets that can be placed on the transmission ring.
Step 23	**protocol** *protocol* {**virtual-template** {*virtual-template-interface-number*}| **dialer**} **Example:** `Router(config-if-atm-vc)# protocol ppp Virutal-Template1`	Configures a static map for an ATM PVC, SVC, or VC class or enables Inverse Address Resolution Protocol (ARP) or Inverse ARP broadcasts on an ATM PVC. In this configuration, the *protocol* argument should be **ppp**. If **ppp** is shown as the *protocol* argument, the **virtual-template** keyword and the *virtual-template-interface-number*argument must be used. The *virtual-template-interface-number* argument may be any number from 1 through 200.
Step 24	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM VC configuration mode.
Step 25	**dsl equipment-type** {**co** | **cpe**} **Example:** `Router(config-if)# dsl co`	Configures the DSL ATM interface to function as central office equipment or customer premises equipment.
Step 26	**dsl operating-mode auto gshdsl symmetric annex** {**A** | **B**} **Example:** `Router(config-if)# dsl operating-mode gshdsl symmetric annex A`	Specifies an operating mode of the digital subscriber line for an ATM interface. **A** specifies North America, and **B** specifies Europe. **A** is the default.
Step 27	**dsl linerate** {*kbps* | **auto**} **Example:** `Router(config-if)# dsl linerate auto`	Specifies a line rate for the DSL ATM interface.
Step 28	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

	Command or Action	Purpose
Step 29	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 30	**ip unnumbered** *type-number* **Example:** `Router(config-if)# ip unnumbered loopback1`	Enables IP processing on a serial interface without assigning an explicit IP address to the interface. **Note** Use Loopback1 for the *type-number*argument. Loopback is a standard configuration for MLP over ATM.
Step 31	**ip tcp header-compression** **Example:** `Router(config-if)# ip tcp header-compression iphc-format`	Enables TCP header compression. **Note** When you use the **show running-config** command, the format of the **ip tcp header-compression**command will change to **ip tcp header-compression iphc-format**.
Step 32	**service-policy** {**input** | **output**} **Example:** `Router(config-if)# service-policy output`	Attaches a policy map to an input interface or virtual circuit (VC), or to an output interface or VC, to be used as the service policy for that interface or VC. For this configuration, use the **output** keyword.
Step 33	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables MLP on an interface and, optionally, enables Bandwidth Allocation Control Protocol (BACP) and Bandwidth Allocation Protocol (BAP) for dynamic bandwidth allocation.
Step 34	**ppp multilink fragment-delay** *delay-max* **Example:** `Router(config-if)# ppp multilink fragment-delay 3`	Specifies a maximum size in units of time for packet fragments on a MLP bundle. The *delay-max* argument is the maximum amount of time, in milliseconds, that it should take to transmit a fragment. The range is from 1 to 1000 milliseconds.
Step 35	**ppp multilink interleave** **Example:** `Router(config-if)# ppp multilink interleave`	Enables interleaving of packets among the fragments of larger packets on a MLP bundle.
Step 36	**ip rtp header-compression** [**passive**] **Example:** `Router(config-if)# ip rtp header-compression passive`	Enables Real-Time Transport Protocol (RTP) header compression. The optional **passive** keyword compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed.

	Command or Action	Purpose
		Note When you enter the **show running-config** command, the format of the **ip rtp header-compression** command will change to **ip rtp header-compression iphc-format**.
Step 37	**ip rtp compression-connections** *number* **Example:** `Router(config-if)# ip rtp compression-connections 3`	Specifies the total number of Real-Time Transport Protocol (RTP) header compression connections that can exist on an interface.
Step 38	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 39	**voice-port** *slot-number* / *subunit-number* / *port* **Example:** `Router(config)# voice-port 0/1/0`	Enters voice-port configuration mode. Enter this command for all ports.
Step 40	**dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**} **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial-peer configuration mode and specifies the method of voice encapsulation, which in this case is POTS**.**
Step 41	**destination-pattern** [+] *string* [**T**] **Example:** `Router(config-dial-peer)# destination-pattern 8...`	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
Step 42	**port** {*slot-number* / *subunit-number* / *port*} **Example:** `Router(config-dial-peer)# port 1/1/0`	Associates a dial peer with a specific voice port.
Step 43	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.

	Command or Action	Purpose
Step 44	**dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**} **Example:** `Router(config)# dial-peer voice 3 voip`	Enters dial-peer configuration mode and specifies the method of voice encapsulation, which in this case is VoIP.
Step 45	**destination-pattern** [+] *string* [**T**] **Example:** `Router(config-dial-peer)# destination-pattern 5...`	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
Step 46	**session target** {**ipv4:** *destination-address*} **Example:** `Router(config-dial-peer)# session target ipv4:192.168.1.1`	Specifies a network-specific address for a specified VoIP dial peer.
Step 47	**dtmf-relay** [**cisco-rtp**] [**h245-alphanumeric**] [**h245-signal**] **Example:** `Router(config-dial-peer)# dtmf-relay cisco-rtp`	Specifies how an H.323 gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network.
Step 48	**ip qos dscp** [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**] **Example:** `Router(config-dial-peer)# ip qos dscp cs5 media`	Specifies IP DSCP. In this case, choose the **media**keyword.
Step 49	**ip qos dscp** [*number* | *set-af* | *set-cs* | **default** | **ef**] [**media** | **signaling**] **Example:** `Router(config-dial-peer)# ip qos dscp cs5 signaling`	Specifies IP DSCP. In this case, choose the **signaling** keyword.
Step 50	**no vad** **Example:** `Router(config-dial-peer)# no vad`	Disables voice activity detection (VAD).

Verifying cRTP Statistics

To display cRTP statistics, use the **show ip rtp header-compression** command as is shown in the following example:

```
Router# show ip rtp header-compression
RTP/UDP/IP header compression statistics:
  Interface Virtual-Template1:
    Rcvf:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs
             0 bytes saved, 0 bytes sent
    Connect: 3 rx slots, 3 tx slots,
             0 long searches, 0 misses 0 collisions, 0 negative cache hits
  Interface Virtual-Access4:
    Rcvf:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs
             0 bytes saved, 0 bytes sent
    Connect: 3 rx slots, 3 tx slots,
             0 long searches, 0 misses 0 collisions, 0 negative cache hits
  Interface Virtual-Access5:
    Rcvf:    7264 total, 7244 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    7414 total, 7392 compressed, 0 status msgs
             280706 bytes saved, 164178 bytes sent
             2.70 efficiency improvement factor
    Connect: 3 rx slots, 3 tx slots,
             0 long searches, 2 misses 1 collisions, 0 negative cache hits
             99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

To display the cRTP gain and to monitor the traffic flow on the actual interface, use the **show interface atm** command.

```
Router# show interface atm 0/0
ATM0/0 is up, line protocol is up
  Hardware is DSLSAR (with Globespan G.SHDSL module)
  MTU 4470 bytes, sub MTU 4470, BW 2304 Kbit, DLY 880 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Encapsulation(s): AAL5 , PVC mode
  23 maximum active VCs, 256 VCs per VP, 1 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  Last input 00:11:57, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: None
  30 second input rate 10000 bits/sec, 50 packets/sec
  30 second output rate 13000 bits/sec, 50 packets/sec
     54153 packets input, 2586202 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     5 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     38013 packets output, 2133672 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuring FRF.5 One-To-One Connections

This task shows you how to configure FRF.5 for a one-to-one connection between two Frame Relay end users over an intermediate ATM network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **frame-relay switching**
4. **interface** *type slot* / *port*
5. **encapsulation frame-relay** [**ietf**]
6. **frame-relay interface-dlci** *dlci* **switched**
7. **frame-relay intf-type** [**dce**]
8. **exit**
9. **interface** *type slot* / *port* . *subinterface-number* {**multipoint** | **point-to-point**}
10. **pvc** *vpi* / *vci*
11. **encapsulation aal5mux frame-relay**
12. **exit**
13. **exit**
14. **connect** *connection-name* {*FR-interface FR-DLCI*} *ATM-interface ATM-VPI* / *VCI* [**network-interworking**]
15. Do one of the following:
    - **clp-bit** {**0** | **1** | **map-de**}
    -
    -
    -
    - **de-bit map-clp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**frame-relay switching** **Example:** `Router(config)# frame-relay switching`	Enables Frame Relay permanent virtual circuit (PVC) switching.

	Command or Action	Purpose
Step 4	**interface** *type slot* / *port* **Example:** `Router(config)# interface serial0`	Enters interface configuration mode.
Step 5	**encapsulation frame-relay** [**ietf**] **Example:** `Router(config-if)# encapsulation frame-relay ietf`	Enables Frame Relay encapsulation. Use the **ietf** keyword to set the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use the **ietf** keyword when connecting to another vendor's equipment across a Frame Relay network.
Step 6	**frame-relay interface-dlci** *dlci* **switched** **Example:** `Router(config-if)# frame-relay interface-dlci 100 switched`	Indicates that a Frame Relay data-link connection identifier (DLCI) is switched and enters Frame Relay dlci configuration mode. The *dlci*argument is the DLCI number to be used on the specified interface or subinterface.
Step 7	**frame-relay intf-type** [**dce**] **Example:** `Router(config-fr-dlci)# frame-relay intf-type dce`	Configures a Frame Relay switch type. Use the **dce** keyword if the router or access server functions as a switch connected to a router.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 9	**interface** *type slot* / *port* . *subinterface-number* {**multipoint** | **point-to-point**} **Example:** `Router(config)# interface atm 1/1.299 multipoint`	Creates an ATM subinterface and enters subinterface configuration mode. The arguments and keywords are as follows: • *type* --Type of interface. Use atm for this configuration. • *slot* --Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information. • *port* --Number of the port being configured. Refer to the appropriate hardware manual for slot and port information. • *subinterface-number* --Subinterface number in the range 1 to 4294967293. The number that precedes the period (**.**) must match the number to which this subinterface belongs. • **multipoint** --Multipoint interface. • **point-to-point** --Point-to-point interface.
Step 10	**pvc** *vpi* / *vci*	Creates an ATM PVC and enters ATM VC configuration mode.

	Command or Action	Purpose
	Example: `Router(config-subif)# pvc 0/1`	The arguments are as follows: • *vpi* / --ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a VPI value defaults the VPI value to 0. • *vci* --ATM network virtual channel identifier (VCI) for this PVC. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. **Note** The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
Step 11	**encapsulation aal5mux frame-relay** **Example:** `Router(config-if-atm-vc)# encapsulation aal5mux frame-relay`	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM permanent virtual circuit (PVC).
Step 12	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM VC configuration mode.
Step 13	**exit** **Example:** `Router(config-subif)# exit`	Exits interface configuration mode.
Step 14	**connect** *connection-name* {*FR-interface FR-DLCI*} *ATM-interface ATM-VPI* / *VCI* [**network-interworking**] **Example:** `Router(config)# connect frf serial0 100 atm 0/33 network-interworking`	Creates a connection to connect the Frame Relay DLCI to the ATM PVC, configures FRF.5 encapsulation, and enters FRF5 configuration mode. The arguments and keywords are as follows: • *connection-name* --Connection name. Enter as a 15-character maximum string. • *FR-interface* --Frame Relay interface type and number, for example, **serial1/0**. • *FR-DLCI* --Frame Relay DLCI in the range from 16 to 1007. • *ATM-interface* --ATM interface type and number, for example, **atm1/0**. • *ATM-VPI* / *VCI* --ATM virtual path identifier/virtual channel identifier (VPI/VCI). If a VPI is not specified, the default VPI is 0. • **network-interworking** --(Optional) FRF.5 network interworking.
Step 15	Do one of the following:	Sets the ATM cell loss priority (CLP) bit field in the ATM cell header.

	Command or Action	Purpose
	• **clp-bit** {**0** | **1** | **map-de**} • • • • **de-bit map-clp** **Example:** `Router(config-frf5)# clp-bit 0`	or Sets the discard eligible (DE) bit mapping from ATM to Frame Relay.

Configuring FRF.5 for Many-To-One Connections

This task shows you how to configure FRF.5 for a many-to-one connection between two Frame Relay end users over an intermediate ATM network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **frame-relay switching**
4. **interface** *type* *slot* / *port*
5. **encapsulation frame-relay** [**ietf**]
6. **frame-relay interface-dlci** *dlci* **switched**
7. **frame-relay intf-type** [**dce**]
8. **exit**
9. **vc-group** *group-name*
10. **interface** *type slot* / *port FR-DLCI FR-SSCS-DLCI*
11. **exit**
12. **interface atm** *slot* / *port* **.** *subinterface-number* {**multipoint** | **point-to-point**}
13. **pvc** *vpi* / *vci*
14. **encapsulation aal5mux frame-relay**
15. **exit**
16. **exit**
17. **connect** *connection-name* **vc-group** *group-name ATM-interface ATM-VPI/VCI*
18. Do one of the following:
    - **clp-bit** {**0** | **1** | **map-de**}
    -
    -
    -
    - **de-bit map-clp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**frame-relay switching** **Example:** `Router(config)# frame-relay switching`	Enables Frame Relay permanent virtual circuit (PVC) switching.
Step 4	**interface** *type slot* / *port* **Example:** `Router(config)# interface serial0`	Enters interface configuration mode.
Step 5	**encapsulation frame-relay** [**ietf**] **Example:** `Router(config-if)# encapsulation frame-relay`	Enables Frame Relay encapsulation. Use the **ietf** keyword to set the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use the **ietf** keyword when connecting to another vendor's equipment across a Frame Relay network.
Step 6	**frame-relay interface-dlci** *dlci* **switched** **Example:** `Router(config-if)# frame-relay interface-dlci 122 switched`	Indicates that a Frame Relay data-link connection identifier (DLCI) is switched and enters Frame Relay dlci configuration mode. The *dlci*argument is the DLCI number to be used on the specified interface or subinterface.
Step 7	**frame-relay intf-type** [**dce**] **Example:** `Router(config-fr-dlci)# frame-relay intf-type dce`	Configures a Frame Relay switch type. Use the **dce** keyword if the router or access server functions as a switch connected to a router.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 9	**vc-group** *group-name* **Example:** `Router(config)# vc-group groupa`	Assigns multiple Frame Relay DLCIs to a VC group and enters ATM-Frame Relay VC group configuration mode.
Step 10	**interface** *type slot* / *port FR-DLCI FR-SSCS-DLCI* **Example:** `Router(config-vc-group)# serial 1/0 100 100`	Specifies the Frame Relay DLCIs in the VC group and maps them to the Frame Relay-SSCS DLCIs.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Router (config-vc-group)# exit`	Exits ATM-Frame Relay VC group configuration mode.
Step 12	**interface atm** *slot* / *port* . *subinterface-number* {**multipoint** | **point-to-point**} **Example:** `Router(config)# interface atm 0/1.22 multipoint`	Creates an ATM subinterface and enters subinterface configuration mode. The arguments and keywords are as follows: • *slot* --Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information. • *port* --Number of the port being configured. Refer to the appropriate hardware manual for slot and port information. • *subinterface-number* --Subinterface number in the range 1 to 4294967293. The number that precedes the period (**.**) must match the number to which this subinterfce belongs. • **multipoint** --Multipoint interface. • **point-to-point** --Point-to-point interface.
Step 13	**pvc** *vpi* / *vci* **Example:** `Router(config-subif)# pvc 0/33`	Creates an ATM permanent virtual circuit (PVC) or assigns a name to an ATM PVC. The arguments are as follows: • *vpi* / --ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a VPI value defaults the VPI value to 0. • *vci* -- ATM network virtual channel identifier (VCI) for this PVC. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
Step 14	**encapsulation aal5mux frame-relay** **Example:** `Router(config-if-atm-vc)# encapsulation aal5mux frame-relay`	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM permanent virtual circuit (PVC) and enters ATM VC configuration mode.
Step 15	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM VC configuration mode.

	Command or Action	Purpose
Step 16	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 17	**connect** *connection-name* **vc-group** *group-name ATM-interface ATM-VPI/VCI* **Example:** `Router(config)# connect frf5-v vc-group groupa atm0 0/33`	Configures an FRF.5 one-to-one connection between two Frame Relay end users over an intermediate ATM network and enters FRF.5 configuration mode. The arguments and keywords are as follows: • *connection-name* --A connection name. Enter as a 15-character maximum string. • **vc-group** --Specifies a VC group name for a many-to-one FRF.5 connection. Enter as an 11- character maximum string. • *ATM-interface* --The ATM interface type and number, for example, **atm1/0**. • *ATM-VPI/VCI* --The ATM virtual path identifier/virtual channel identifier (VPI/VCI). If a VPI is not specified, the default VPI is 0.
Step 18	Do one of the following: • **clp-bit** {**0** | **1** | **map-de**} • • • • **de-bit map-clp** **Example:** `Router(config-frf5)# clp-bit 0`	Sets the ATM cell loss priority (CLP) bit field in the ATM cell header. or Sets the discard eligible (DE) bit mapping from ATM to Frame Relay.

Verifying FRF.5

The following **show** command output is from a Cisco 1721 router. Use the **show connection all** or **show connection id** commands to check the state of the connection. Use the **show frame-relay pvc** command to verify the state of the Frame Relay PVC, and use the **show atm pvc** command to verify the state of the ATM PVC.

```
Router# show connection all
ID   Name               Segment 1            Segment 2           State
========================================================================
```

```
1    frf5              Serial0 100          ATM0 0/33            UP
Router# show connection id
 1
FR/ATM Network Interworking Connection: frf5
  Status    - UP
  Segment 1 - Serial0 DLCI 100
  Segment 2 - ATM0 VPI 0 VCI 33
  Interworking Parameters -
    fr-sscs-dlci 1022
    de-bit map-clp
    clp-bit map-de
Router# show frame-relay pvc 100
PVC Statistics for interface Serial0 (Frame Relay DCE)
DLCI = 100, DLCI USAGE = FRF.5, PVC STATUS = ACTIVE, INTERFACE = Serial0
  input pkts 5             output pkts 5            in bytes 520
  out bytes 520            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  switched pkts 5
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 00:25:00, last time pvc status changed 00:05:16
Router# show atm pvc 0/33
ATM0.1: VCf: 1, VPI: 0, VCI: 33
UBR, PeakRate: 2304
AAL5-FRATM, etype:0x3, Flags: 0xC22, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM END CC Activate retry count: 3, OAM END CC Deactivate retry count: 3
OAM END CC retry frequency: 30 second(s),
OAM SEGMENT CC Activate retry count: 3, OAM SEGMENT CC Deactivate retry count: 3
OAM SEGMENT CC retry frequency: 30 second(s),
OAM Loopback status: OAM Disabled
OAM VC state: Not Managed
ILMI VC state: Not Managed
InARP DISABLED
InPkts: 5, OutPkts: 5, InBytes: 540, OutBytes: 540
InPRoc: 0, OutPRoc: 0
InFast: 5, OutFast: 5, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0/0/0 (holdq/outputq/total)
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0
OAM cells receivef: 0
F5 InEndloop: 0, F5 InSegloop: 0,
F5 InEndcc: 0, F5 InSegcc: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0,
F5 OutEndcc: 0, F5 OutSegcc: 0, F5 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

Configuring FRF.8

This task shows you how to configure FRF.8.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **frame-relay switching**
4. **interface serial** *slot* / *port*
5. **encapsulation frame-relay [ietf]**
6. **no fair-queue**
7. **frame-relay interface-dlci** *dlci* **switched**
8. **frame-relay intf-type dce**
9. **exit**
10. **interface** *type slot* / *port* . *subinterface-number* {**multipoint** | **point-to-point**}
11. **pvc** *vpi* / *vci*
12. **encapsulation aal5mux fr-atm-srv**
13. **exit**
14. **exit**
15. **connect** *connection-name FR-interface FR-DLCI ATM-interface ATM-VPI/VCI* **service-interworking**
16. Do one of the following:
    - **clp-bit** {**0** | **1** | **map-de**}
    -
    -
    - **de-bit** {**0** | **1** | **map-clp**}
    -
    -
    - **efci-bit** {**0** | **map-fecn**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**frame-relay switching** **Example:** `Router(config)# frame-relay switching`	Enables Frame Relay permanent virtual circuit (PVC) switching.
Step 4	**interface serial** *slot* / *port* **Example:** `Router(config)# interface serial 0/1`	Enters interface configuration mode.
Step 5	**encapsulation frame-relay [ietf]** **Example:** `Router(config-if)# encapsulation frame-relay ietf`	Enables Frame Relay encapsulation. Use the **ietf** keyword to set the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.
Step 6	**no fair-queue** **Example:** `Router(config-if)# no fair-queue`	Deletes the configured number of queues from the traffic class.
Step 7	**frame-relay interface-dlci** *dlci* **switched** **Example:** `Router(config-if)# frame-relay interface-dlci 199 switched`	Indicates that a Frame Relay data-link connection identifier (DLCI) is switched and enters Frame Relay dlci configuration mode. The *dlci*argument is the DLCI number to be used on the specified interface or subinterface.
Step 8	**frame-relay intf-type dce** **Example:** `Router(config-fr-dlci)# frame-relay intf-type dce`	Configures a Frame Relay switch type. Use the **dce** keyword if the router or access server functions as a switch connected to a router.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 10	**interface** *type slot* / *port* **.** *subinterface-number* {**multipoint** | **point-to-point**} **Example:** `Router(config)# interface atm 0/1.299 multipoint`	Configures an interface type and enters subinterface configuration mode. The arguments and keywords are as follows: • *type* --To configure FRF.8, use atm for the *type* argument. • *slot* --Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.

	Command or Action	Purpose
		• *port* --Number of the port being configured. Refer to the appropriate hardware manual for slot and port information. • *subinterface-number* --Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs. • **multipoint** --Multipoint interface. • **point-to-point** --Point-to-point interface.
Step 11	**pvc** *vpi* / *vci* **Example:** `Router(config-subif)# pvc 1/1`	Creates an ATM PVC, assigns a name to an ATM PVC, and enters ATM VC configuration mode. The arguments are as follows: • *vpi* / --ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a VPI value defaults the VPI value to 0. • *vci* --ATM network virtual channel identifier (VCI) for this PVC. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
Step 12	**encapsulation aal5mux fr-atm-srv** **Example:** `Router(config-if-atm-vc)# encapsulation aal5mux fr-atm-srv`	Configures the ATM adaptation layer (AAL) and encapsulation type for an ATM PVC.
Step 13	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM VC configuration mode.
Step 14	**exit** **Example:** `Router(config-if) exit`	Exits interface configuration mode.
Step 15	**connect** *connection-name FR-interface FR-DLCI ATM-interface ATM-VPI/VCI* **service-interworking**	Configures an FRF.8 one-to-one mapping between a Frame Relay DLCI and an ATM permanent virtual circuit (PVC) and enters FRF.8 configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# connect frf8 serial0 100 atm0 0/33 service-interworking`	The arguments and keywords are as follows: • *connection-name* --Connection name. Enter as a 15-character maximum string. • *FR-interface* --Frame Relay interface type and number, for example, **serial1/0**. • *FR-DLCI* --Frame Relay data-link connection identifier (DLCI) in the range 16 to 1007. • *ATM-interface* -- ATM interface type and number, for example **atm1/0**. • *ATM-VPI/VCI* --ATM virtual path identifier/virtual channel identifier (VPI/VCI). If a VPI is not specified, the default VPI is 0. • **service-interworking** --FRF.8 service interworking.
Step 16	Do one of the following: • **clp-bit** {**0** | **1** | **map-de**} • • • **de-bit** {**0** | **1** | **map-clp**} • • • **efci-bit** {**0** | **map-fecn**} **Example:** `Router(config-frf8)# clp-bit 0`	Sets the ATM cell loss priority (CLP) bit field in the ATM cell header. or Sets the Frame Relay discard eligible (DE) bit field in the Frame Relay header. or Sets the explicit forward congestion indication (EFCI) bit field in the ATM cell header.

Verifying FRF.8

The following **show** command output is from a Cisco 1721 router. Use the **show connection all** or **show connection id** commands to check the state of the connection. Use **show frame-relay pvc** command to verify the state of the Frame Relay PVC and use **show atm pvc command**to verify the state of the ATM PVC.

```
Router# show connection all
ID   Name               Segment 1            Segment 2           State
========================================================================
2    frf8              Serial0 100          ATM0 0/33           UP
Router# show connection id 2
FR/ATM Service Interworking Connection: frf8
  Status    - UP
  Segment 1 - Serial0 DLCI 100
  Segment 2 - ATM0 VPI 0 VCI 33
```

```
Interworking Parameters -
    service translation
    efci-bit 0
    de-bit map-clp
    clp-bit map-de
Router# show frame-relay pvc
PVC Statistics for interface Serial0 (Frame Relay DCE)
              Active     Inactive      Deleted       Static
  Local          0            0            0            0
  Switched       1            0            0            0
  Unused         0            0            0            0
DLCI = 100, DLCI USAGE = FRF.8, PVC STATUS = ACTIVE, INTERFACE = Serial0
  input pkts 5             output pkts 5             in bytes 540
  out bytes 520            dropped pkts 0            in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0            out FECN pkts 0
  out BECN pkts 0          in DE pkts 0              out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  switched pkts 5
  Detailed packet drop counters:
  no out intf 0            out intf down 0           no out PVC 0
  in PVC down 0            out PVC down 0            pkt too big 0
  shaping Q full 0         pkt above DE 0            policing drop 0
  pvc create time 00:08:57, last time pvc status changed 00:08:20
Router# show atm pvc 0/33
ATM0.1: VCf: 1, VPI: 0, VCI: 33
UBR, PeakRate: 2304
AAL5-FRATMSRV, etype:0x15, Flags: 0xC23, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM END CC Activate retry count: 3, OAM END CC Deactivate retry count: 3
OAM END CC retry frequency: 30 second(s),
OAM SEGMENT CC Activate retry count: 3, OAM SEGMENT CC Deactivate retry count: 3
OAM SEGMENT CC retry frequency: 30 second(s),
OAM Loopback status: OAM Disabled
OAM VC state: Not Managed
ILMI VC state: Not Managed
InARP DISABLED
InPkts: 5, OutPkts: 5, InBytes: 560, OutBytes: 560
InPRoc: 0, OutPRoc: 0
InFast: 5, OutFast: 5, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0/0/0 (holdq/outputq/total)
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0
OAM cells receivef: 0
F5 InEndloop: 0, F5 InSegloop: 0,
F5 InEndcc: 0, F5 InSegcc: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0,
F5 OutEndcc: 0, F5 OutSegcc: 0, F5 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

Configuring MLP Bundling

This task shows you how to configure MLP bundling using a multilink interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multilink** *multilink-bundle-number*
4. **ip address** *ip-address mask* [**secondary**]
5. **service-policy** {**input** | **output**} *policy-map-name*
6. **ppp multilink**
7. **ppp multilink fragment-delay** *delay-max*
8. **ppp multilink interleave**
9. **interface virtual-template** *number*
10. **no ip address**
11. **ppp multilink**
12. **ppp multilink multiclass**
13. **ppp multilink group** *group-number*
14. **exit**
15. **interface** *type slot* / *port* . *subinterface-number* [**point-to-point**]
16. **pvc** *vpi* / *vci*
17. **vbr-rt** *peak-rate average-rate burst*
18. **tx-ring-limit** *ring-limit*
19. **protocol** *protocol protocol-address*
20. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface multilink** *multilink-bundle-number* **Example:** `Router(config)# interface multilink1`	Creates a multilink bundle or enters multilink interface configuration mode. The *multilink-bundle-number* argument is the number of the multilink bundle (a nonzero number).

	Command or Action	Purpose
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 172.10.10.0`	Sets a primary or secondary IP address for an interface.
Step 5	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy output green`	Attaches a policy map to an input interface or virtual circuit (VC), or to an output interface or VC, to be used as the service policy for that interface or VC.
Step 6	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables Multilink PPP (MLP) on an interface and, optionally, enables Bandwidth Allocation Control Protocol (BACP) and Bandwidth Allocation Protocol (BAP) for dynamic bandwidth allocation.
Step 7	**ppp multilink fragment-delay** *delay-max* **Example:** `Router(config-if)# ppp multilink fragment-delay 10`	Specifies a maximum size in units of time for packet fragments on a MLP bundle. The *delay-max* argument is the maximum amount of time, in milliseconds, that it should take to transmit a fragment. The range is from 1 to 1000 milliseconds.
Step 8	**ppp multilink interleave** **Example:** `Router(config-if)# ppp multilink interleave`	Enables interleaving of packets among the fragments of larger packets on an MLP bundle.
Step 9	**interface virtual-template** *number* **Example:** **Example:** `Router(config)# interface virtual-template10`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode. The *number* argument is the number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured.
Step 10	**no ip address** **Example:** `Router(config-if)#` **no ip address**	Removes an IP address or disables IP processing.

	Command or Action	Purpose
Step 11	**ppp multilink** **Example:** `Router(config-if)#` **ppp multilink**	Enables MLP on an interface and, optionally, enables BACP and BAP for dynamic bandwidth allocation..
Step 12	**ppp multilink multiclass** **Example:** `Router(config-if)#` **ppp multilink multiclass**	Allows interleaving to be used on bundles that consist of more than one link. For Point-to-Point Protocol over ATM (PPPoA) and Point-to-Point Protocol over Frame Relay (PPPoFR), the command is entered on the virtual template.
Step 13	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink group 299`	Restricts a physical link to joining only a designated multilink-group interface. The *group-number* argument is a multilink-group number (a nonzero number).
Step 14	**exit** **Example:** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 15	**interface** *type slot* / *port* . *subinterface-number* [**point-to-point**] **Example:** `Router(config)# interface atm 0/1.299`	Configures an interface type and enters interface configuration mode. The *type* argument should be ATM.
Step 16	**pvc** *vpi* / *vci* **Example:** `Router(config-if)# pvc 1/0`	Creates an ATM PVC or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode.
Step 17	**vbr-rt** *peak-rate average-rate burst* **Example:** `Router(config-if-atm-vc)# vbr-rt 640 640`	Configures the real-time variable bit rate (VBR) for Voice over ATM connections.

	Command or Action	Purpose
Step 18	**tx-ring-limit** *ring-limit* **Example:** `Router(config-if-atm-vc)# tx-ring-limit 55`	Limits the number of packets that can be used on a transmission ring on the PVC. The *ring-limit* argument is the maximum number of allowable packets that can be placed on the transmission ring. The default value is 60. On Cisco 1700 series routers, possible values are 1 through 60. On Cisco 2600 and Cisco 3600 series routers, possible values are 3 through 60.
Step 19	**protocol** *protocol protocol-address* **Example:** `Router(config-if-atm-vc)# protocol ppp virtual-template1`	Configures a static map for an ATM PVC, switched virtual circuit (SVC), or VC class or enables Inverse Address Resolution Protocol (ARP) or Inverse ARP broadcasts on an ATM PVC. The *protocol* argument should be PPP. The *protocol-address*argument should be virtual-template1 (the destination address that is being mapped to a PVC).
Step 20	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits interface ATM VC configuration mode. **Note** Repeat Steps 13 through 18 to create another MLP bundle.

Verifying MLP Bundling

To verify your MLP bundling configuration, use the following **show** commands:

```
Router# show ppp multilink
Multilink1, bundle name is 3660
  Bundle up for 00:00:17E, 1/255 load, 2 receive classes, 2 transmit classes
  Receive Class 0:
    1 lost fragments, 1 reordered, 0 unassigned
    0 discarded, 0 lost received
    0x3 received sequence
  Receive Class 1:
    0 lost fragments, 0 reordered, 0 unassigned
    0 discarded, 0 lost received
    0x0 received sequence
  Transmit Class 0:
    0x2 sent sequence
  Transmit Class 1:
    0x0 sent sequence
  Member links: 2 active, 5 inactive (max not set, min not set)
    Vi8, since 00:00:17  480 weight, 472 frag size
    Vi9, since 00:00:17  480 weight, 472 frag size
Router# show interfaces multilink 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Interface is unnumbered. Using address of Loopback0 (2.2.2.2)
  MTU 1500 bytes, BW 1280 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, loopback not set
  DTR is pulsed for 2 seconds on reset
  Last input 02:57:52, output never, output hang never
```

```
  Last clearing of "show interface" counters 02:58:45
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 860 kilobits/sec
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     2 packets input, 28 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     2 packets output, 24 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
Router# show interfaces atm 0/0
ATM0/0 is up, line protocol is up
  Hardware is DSLSAR (with Alcatel ADSL Module)
  MTU 4470 bytes, sub MTU 4470, BW 800 Kbit, DLY 2560 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Encapsulation(s): AAL5  AAL2, PVC mode
  23 maximum active VCs, 256 VCs per VP, 1 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: None
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     2188 packets input, 30640 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     4 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     2194 packets output, 48368 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Router# show users
   Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
  Interface    User               Mode          Idle      Peer Address
  Vi4          3660           PPPoATM      00:09:25
  Vi5          3660           PPPoATM      00:09:23
  Mu1        3660              Sync PPP     00:09:25  2.2.2.2
Router# show policy-map interface mul 1
 Multilink1
  Service-policy output: CISCO
    Class-map: VOICE (match-all)
      11117 packets, 234235 bytes
      30 second offered rate 25000 bps, drop rate 0 bps
      Match: access-group 100
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 100 (kbps) Burst 2500 (Bytes)
        (pkts matched/bytes matched) 17/748
        (total drops/bytes drops) 0/0
    Class-map: class-default (match-any)
      234453438 packets, 64564574574bytes
      30 second offered rate 645000 bps, drop rate 12000 bps
      Match: any
Router# show dsl interface atm 0/0
Alcatel 20150 chipset information
                ATU-R (DS)                      ATU-C (US)
Modem Status:    Showtime (DMTDSL_SHOWTIME)
DSL Mode:        ITU G.992.1 (G.DMT)
ITU STD NUM:     0x01                            0x1
Vendor If:       'ALCB'                          'GSPN'
Vendor Specific: 0x0000                          0x0002
Vendor Country:  0x00                            0x00
Capacity Usef:   80%                             90%
Noise Margin:    11.5 dB                          9.0 dB
```

```
Output Power:     8.0 dBm                       12.0 dBm
Attenuation:      0.0 dB                         4.0 dB
Defect Status:   None                          None
Last Fail Code:  Handshake or init message invalid or had bad CRC
Selftest Result: 0x00
Subfunction:     0x15
Interrupts:      1333 (0 spurious)
PHY Access Err:  0
Activations:     1
Init FW:         embedded
Operation FW:    embedded
SW Version:      3.8129
FW Version:      0x1A04
                 Interleave             Fast    Interleave              Fast
Speed (kbps):          7616                0           800                 0
Reed-Solomon EC:          4                0          1326                 0
CRC Errors:               0                0             1                 0
Header Errors:            0                0             0                 0
Bit Errors:               0                0
BER Valid sec:            0                0
BER Invalid sec:          0                0
DMT Bits Per Bin
00: 0 0 0 0 0 0 0 0 6 7 8 9 9 B B C C
10: B B C C B B A 9 9 9 9 8 8 9 0 0
20: 0 0 0 0 0 0 3 4 4 5 6 6 7 7 7 8
30: 8 8 9 9 9 9 A A A A A A A A 9 A
40: 0 B B B B B B B B B B B B B B B
50: B B B B B B B B B B B B B 8 B 2
60: B B B B B B B B B B B B B B B B
70: B B B B B B 8 B B B B B 9 B B B
80: B B B B B B B B B B B B B B B B
90: B B B B B B B B B B B B 9 B B B
A0: B B B B B B B B B B B B B B B B
B0: B B B B B B B A B B A 9 A A A A
C0: A A A A A A A A A A A A A A A A
D0: A A A A A A A A A A 9 A A A A A
E0: A A A A A A 9 A 9 9 8 8 7 5 5 5
F0: 4 3 2 0 0 0 0 0 0 0 0 0 0 0 0 0

DSL: Training log buffer capability is not enabled
```

Troubleshooting Tips for MLP Bundling

To troubleshoot your MLP bundling configuration, do the following:

SUMMARY STEPS

1. Verify the status of the multilink interface using the **show interface multilink** command.
2. If a multilink member is inactive, verify the status of the ATM interface using the **show interface atm**command.
3. Check all Link Control Protocol (LCP) and Network Control Program (NCP) negotiation messages using the **debug ppp negotiation** command (see the following output example).
4. Check all Challenge Handshake Authentication Protocol (CHAP) authentication messages using the **debug ppp authentication** command (see the following output example).
5. Check all MLP bundle events using the **debug ppp multilink events** command (see the following output example).

DETAILED STEPS

Step 1 Verify the status of the multilink interface using the **show interface multilink** command.

- If the multilink interface is down, verify the status of all multilink bundle members using the **show ppp multilink**command.
- If the multilink line protocol is down, verify the Network Control Protocol (NCP) and MLP messages using the **debug ppp negotiation** and **debug ppp multilink events**commands.

Step 2 If a multilink member is inactive, verify the status of the ATM interface using the **show interface atm**command.

- If the ATM interface is down, verify the status of the corresponding DSL link using the **show dsl interface atm**command.

Step 3 Check all Link Control Protocol (LCP) and Network Control Program (NCP) negotiation messages using the **debug ppp negotiation** command (see the following output example).

Example:

```
Router# debug ppp negotiation
1d05h: ppp11 LCP: State is Open
1d05h: ppp11 PPP: Phase is FORWARDING, Attempting Forward
1d05h: Vi7 PPP: Phase is DOWN, Setup
1d05h: Vi7 PPP: Phase is DOWN, Setup
1d05h: ppp11 LCP: I TERMREQ [Open] id 2 len 4
1d05h: ppp11 LCP: O TERMACK [Open] id 2 len 4
1d05h: ppp11 PPP: Phase is TERMINATING
1d05h: ppp13 PPP: Treating connection as a dedicated line
1d05h: ppp13 PPP: Phase is ESTABLISHING, Active Open
1d05h: ppp13 LCP: O CONFREQ [Closed] id 1 len 29
1d05h: ppp13 LCP:    MagicNumber 0x0FD2BAA3 (0x05060FD2BAA3)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 PPP: Treating connection as a dedicated line
1d05h: ppp14 PPP: Phase is ESTABLISHING, Active Open
1d05h: ppp14 LCP: O CONFREQ [Closed] id 1 len 29
1d05h: ppp14 LCP:    MagicNumber 0x0FD2BB2D (0x05060FD2BB2D)
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: TIMEout: State REQsent
1d05h: ppp13 LCP: O CONFREQ [REQsent] id 2 len 29
1d05h: ppp13 LCP:    MagicNumber 0x0FD2BAA3 (0x05060FD2BAA3)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 LCP: TIMEout: State REQsent
1d05h: ppp14 LCP: O CONFREQ [REQsent] id 2 len 29
1d05h: ppp14 LCP:    MagicNumber 0x0FD2BB2D (0x05060FD2BB2D)
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: TIMEout: State REQsent
1d05h: ppp13 LCP: O CONFREQ [REQsent] id 3 len 29
1d05h: ppp13 LCP:    MagicNumber 0x0FD2BAA3 (0x05060FD2BAA3)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 LCP: TIMEout: State REQsent
1d05h: ppp14 LCP: O CONFREQ [REQsent] id 3 len 29
1d05h: ppp14 LCP:    MagicNumber 0x0FD2BB2D (0x05060FD2BB2D)
```

```
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: TIMEout: State REQsent
1d05h: ppp13 LCP: O CONFREQ [REQsent] id 4 len 29
1d05h: ppp13 LCP:    MagicNumber 0x0FD2BAA3 (0x05060FD2BAA3)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 LCP: TIMEout: State REQsent
1d05h: ppp14 LCP: O CONFREQ [REQsent] id 4 len 29
1d05h: ppp14 LCP:    MagicNumber 0x0FD2BB2D (0x05060FD2BB2D)
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: I CONFREQ [REQsent] id 1 len 29
1d05h: ppp13 LCP:    MagicNumber 0x36EBFBB7 (0x050636EBFBB7)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 3660 (0x130B01333636302D746F70)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: O CONFACK [REQsent] id 1 len 29
1d05h: ppp13 LCP:    MagicNumber 0x36EBFBB7 (0x050636EBFBB7)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 3660 (0x130B01333636302D746F70)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 LCP: I CONFREQ [REQsent] id 1 len 29
1d05h: ppp14 LCP:    MagicNumber 0x36EBFBB8 (0x050636EBFBB8)
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 3660 (0x130B01333636302D746F70)
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 LCP: O CONFACK [REQsent] id 1 len 29
1d05h: ppp14 LCP:    MagicNumber 0x36EBFBB8 (0x050636EBFBB8)
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 3660 (0x130B01333636302D746F70)
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: TIMEout: State ACKsent
1d05h: ppp13 LCP: O CONFREQ [ACKsent] id 5 len 29
1d05h: ppp13 LCP:    MagicNumber 0x0FD2BAA3 (0x05060FD2BAA3)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: I CONFACK [ACKsent] id 5 len 29
1d05h: ppp13 LCP:    MagicNumber 0x0FD2BAA3 (0x05060FD2BAA3)
1d05h: ppp13 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp13 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp13 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp13 LCP: State is Open
1d05h: ppp13 PPP: Phase is FORWARDING, Attempting Forward
1d05h: Vi8 PPP: Phase is DOWN, Setup
1d05h: Vi8 PPP: Phase is DOWN, Setup
1d05h: ppp13 PPP MLP: Queue packet code[192] id[0]
1d05h: %LINK-3-UPDOWN: Interface Virtual-Access8, changed state to up
1d05h: Vi8 PPP: Phase is ESTABLISHING, Finish LCP
1d05h: Vi8 PPP: Phase is VIRTUALIZED
1d05h: Mu1 MLP: Added first link Vi8 to bundle 3660
1d05h: Vi8 PPP: Process pending packets
1d05h: Vi8 MLP: Redirect packet to MLP
1d05h: %LINK-3-UPDOWN: Interface Multilink1, changed state to up
1d05h: Mu1 PPP: Phase is UP
1d05h: Mu1 IPCP: O CONFREQ [Closed] id 2 len 10
1d05h: Mu1 IPCP:    Address 2.2.2.2 (0x030602020202)
1d05h: Mu1 PPP: Process pending packets
1d05h: Mu1 PPP: Process pending packets
1d05h: Mu1 PPP: Treating connection as a dedicated line
1d05h: Mu1 IPCP: I CONFACK [REQsent] id 2 len 10
1d05h: Mu1 IPCP:    Address 2.2.2.2 (0x030602020202)
1d05h: ppp14 LCP: TIMEout: State ACKsent
1d05h: ppp14 LCP: O CONFREQ [ACKsent] id 5 len 29
1d05h: ppp14 LCP:    MagicNumber 0x0FD2BB2D (0x05060FD2BB2D)
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
```

```
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 LCP: I CONFACK [ACKsent] id 5 len 29
1d05h: ppp14 LCP:    MagicNumber 0x0FD2BB2D (0x05060FD2BB2D)
1d05h: ppp14 LCP:    MRRU 1524 (0x110405F4)
1d05h: ppp14 LCP:    EndpointDisc 1 2600 (0x130B0132363531584D2D31)
1d05h: ppp14 LCP:    MultilinkHdrFmt seq long classes 2 (0x1B040202)
1d05h: ppp14 LCP: State is Open
1d05h: ppp14 PPP: Phase is FORWARDING, Attempting Forward
1d05h: Vi9 PPP: Phase is DOWN, Setup
1d05h: Vi9 PPP: Phase is DOWN, Setup
1d05h: %LINK-3-UPDOWN: Interface Virtual-Access9, changed state to up
1d05h: Vi9 PPP: Phase is ESTABLISHING, Finish LCP
 1d05h: Vi9 PPP: Phase is VIRTUALIZED
1d05h: Mu1 MLP: Added link Vi9 to bundle 3660
1d05h: Vi9 PPP: Process pending packets
1d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access8, changed state to up
1d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Multilink1, changed state to up
1d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access9, changed state to up
1d05h: Mu1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
1d05h: Mu1 IPCP:    Address 2.2.2.3 (0x030602020203)
1d05h: Mu1 AAA/AUTHOR/IPCP: Start.  Her address 2.2.2.3, we want 0.0.0.0
1d05h: Mu1 AAA/AUTHOR/IPCP: Reject 2.2.2.3, using 0.0.0.0
1d05h: Mu1 AAA/AUTHOR/IPCP: Done.  Her address 2.2.2.3, we want 0.0.0.0
1d05h: Mu1 IPCP: O CONFACK [ACKrcvd] id 8 len 10
1d05h: Mu1 IPCP:    Address 2.2.2.3 (0x030602020203)
1d05h: Mu1 IPCP: State is Open
1d05h: Mu1 IPCP: Install route to 2.2.2.3
1d05h: Mu1 IPCP: Add link info for cef entry 2.2.2.3
```

Step 4 Check all Challenge Handshake Authentication Protocol (CHAP) authentication messages using the **debug ppp authentication** command (see the following output example).

Example:

```
Router# debug ppp authentication
1d06h: ppp295 PPP: Treating connection as a dedicated line
1d06h: ppp295 PPP: Authorization required
1d06h: ppp296 PPP: Treating connection as a dedicated line
1d06h: ppp296 PPP: Authorization required
1d06h: ppp295 CHAP: O CHALLENGE id 1 len 29 from "3660"
1d06h: ppp295 CHAP: I CHALLENGE id 1 len 29 from "2600"
1d06h: ppp295 CHAP: Using hostname from unknown source
1d06h: ppp295 CHAP: Using password from AAA
1d06h: ppp295 CHAP: O RESPONSE id 1 len 29 from "3660"
1d06h: ppp295 CHAP: I RESPONSE id 1 len 29 from "2600"
1d06h: ppp295 PPP: Sent CHAP LOGIN Request
1d06h: ppp295 PPP: Received LOGIN Response PASS
1d06h: %LINK-3-UPDOWN: Interface Virtual-Access4, changed state to up
1d06h: Vi4 CHAP: O SUCCESS id 1 len 4
1d06h: Vi4 CHAP: I SUCCESS id 1 len 4
1d06h: %LINK-3-UPDOWN: Interface Multilink1, changed state to up
1d06h: Mu1 PPP: Treating connection as a dedicated line
1d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access4, changed state to up
1d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Multilink1, changed state to up
1d06h: ppp296 CHAP: O CHALLENGE id 1 len 29 from "3660" ç
1d06h: ppp296 CHAP: I CHALLENGE id 1 len 29 from "2600" ç
1d06h: ppp296 CHAP: Using hostname from unknown source
1d06h: ppp296 CHAP: Using password from AAA
1d06h: ppp296 CHAP: O RESPONSE id 1 len 29 from "3660"
1d06h: ppp296 CHAP: I RESPONSE id 1 len 29 from "2600"
1d06h: ppp296 PPP: Sent CHAP LOGIN Request
1d06h: ppp296 PPP: Received LOGIN Response PASS ç
1d06h: %LINK-3-UPDOWN: Interface Virtual-Access5, changed state to up
1d06h: Vi5 CHAP: O SUCCESS id 1 len 4
1d06h: Vi5 CHAP: I SUCCESS id 1 len 4
1d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access5, changed state to up
```

Step 5 Check all MLP bundle events using the **debug ppp multilink events** command (see the following output example).

Example:

```
Router# debug ppp multilink events
1d05h: %LINK-3-UPDOWN: Interface Virtual-Access8, changed state to up
1d05h: %LINK-3-UPDOWN: Interface Virtual-Access9, changed state to up
1d05h: Vi8 MLP: Request add link to bundle
1d05h: Vi9 MLP: Request add link to bundle
1d05h: Vi8 MLP: Adding link to bundle
1d05h: Mu1 MLP: Added first link Vi8 to bundle 3660 1d05h: Vi9 MLP: Adding link to bundle
1d05h: Mu1 MLP: Added link Vi9 to bundle 3660
1d05h: %LINK-3-UPDOWN: Interface Multilink1, changed state to up
1d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access8, changed state to up
1d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access9, changed state to up
1d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Multilink1, changed st
```

Configuring the Tx Ring Limit

This task shows you how to configure the tx ring limit.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *port*
4. **pvc** [*name*] *vpi* / *vci*
5. Do one of the following:
   - **vbr-rt** *peak-rate average-rate burst*
   -
   -
   - **vbr-nrt** *output-pcr output-scr output-mbs* [*input-pcr*] [*input-scr*] [*input-mbs*]
6. **tx-ring-limit** *ring-limit*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *port* **Example:** `Router(config)# interface atm 0/1`	Configures an ATM interface type and enters interface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 1/1`	Creates an ATM permanent virtual circuit (PVC) or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode.
Step 5	Do one of the following: • **vbr-rt** *peak-rate average-rate burst* • • • **vbr-nrt** *output-pcr output-scr output-mbs* [*input-pcr*] [*input-scr*] [*input-mbs*] **Example:** `Router(config-if-atm-vc)# vbr-rt 640 640`	Configures the real-time variable bit rate (VBR) for Voice over ATM connections. or Configures the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specifies output peak cell rate (PCR), output sustainable cell rate (SCR), and output maximum burst cell size for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), VC class, or VC bundle member. **Note** The **tx-ring-limit** command needs to be used with either the **vbr-rt** command or the **vbr-nrt** command and also in conjunction with low latency queueing (LLQ).
Step 6	**tx-ring-limit** *ring-limit* **Example:** `Router(config-if-atm-vc)# tx-ring-limit 3`	Limits the number of packets that can be used on a transmission ring on the permanent virtual circuit (PVC). The argument is as follows: • *ring-limit* --Maximum number of allowable packets that can be placed on the transmission ring. The default value is 60. On Cisco 1700 series routers, possible values are 1 through 60. On Cisco 2600 and Cisco 3600 series routers, possible values are 3 through 60.

Verifying the Tx Ring Limit

The following output example is for a tx ring limit over ADSL configuration:

```
Router# show running-config

interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 pvc 1/100
  vbr-rt 1500 1500
  tx-ring-limit 3
  protocol ppp Virtual-Template1
 !
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
```

Configuration Examples

ATM CLP Bit Marking over G.SHDSL Example

The following output is from a Cisco 1721 router. In this example, all output packets that have an IP precedence value of 0 are sent with the CLP set to 1.

Note IP Cisco Express Forwarding (IP CEF) must be turned on using the **ip cef** command-line interface before ATM CLP bit marking is configured.

- ATM CLP bit marking can be applied only as output policy for an interface.

```
ip cef
!
class-map match-all PREC0
 match ip precedence 0
!
policy-map ATM_CLP
 class PREC0
  set atm-clp
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
!
interface ATM0.1 point-to-point
 ip address 10.0.0.1 255.255.255.0
 pvc 0/33
  service-policy output ATM_CLP
```

Clock Rate for ADSL and G.SHDSL WICs Example

The following example from a Cisco 1760 router shows that the clock rate on the AAL5 channel is set to the minimum value of 4 Mbps on interface ATM 0/0:

```
interface atm 0/0
 clock rate aal5 4000000
```

The following example from a Cisco 1760 router shows that the clock rate on the AAL2 channel is set to the value of 5.3 Mbps on interface ATM 1/0:

```
interface atm 1/0
 clock rate aal2 5300000
```

The following example from a Cisco 2621 mainboard module shows that the clock rate on the AAL5 channel is set to the maximum value of 7 Mbps on interface ATM 0/0:

```
interface atm 0/0
 clock rate aal5 7000000
```

The following example from a Cisco 2621 network module shows that the clock rate on the AAL5 channel is set to the maximum value of 5.3 Mbps on interface ATM 1/0:

```
interface atm 1/0
 clock rate aal5 5300000
```

cRTP over an ATM Link with PPP Encapsulation Example

The following example shows that cRTP has been configured using Virtual Template over ATM:

```
ip cef
class-map match-all voice-traffic
 match access-group 102
class-map match-all voice-signalling
 match access-group 103
!
policy-map VOICE-POLICY
 class voice-traffic
  priority 48
 class voice-signalling
  bandwidth 8
 class class-default
  fair-queue
!
interface Loopback0
 ip address 192.168.1.2 255.255.255.0
!
interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 pvc 1/100
  vbr-rt 1500 1500
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip tcp header-compression iphc-format
 service-policy output VOICE-POLICY
```

```
 ppp multilink
 ppp multilink fragment-delay 3
 ppp multilink interleave
 ip rtp header-compression iphc-format
 ip rtp compression-connections 3
!
access-list 102 permit udp any any range 16384 37276
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer voice 1 pots
 destination-pattern 7...
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 8...
 session target ipv4:192.168.1.1
dtmf-relay cisco-rtp
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
```

FRF.5 over G.SHDSL Example

The following output is from a Cisco 1721 router. This example shows how to create an FRF.5 one-to-one connection using the the **connect** command with the **network-interworking** keyword.

```
frame-relay switching
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
!
interface ATM0.1 point-to-point
 pvc 0/33
  encapsulation aal5mux frame-relay
!
interface Serial0
 no ip address
 encapsulation frame-relay IETF
 clockrate 2000000
 frame-relay interface-dlci 100 switched
 frame-relay intf-type dce
!
connect frf5 Serial0 100 ATM0 0/33 network-interworking
!
```

The following example shows how to create an FRF.5 many-to-one connection.

```
vc-group groupA
 Serial0 100 100
 Serial0 200 200
 Serial0 300 300
 Serial0 400 400
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 0/33
  encapsulation aal5mux frame-relay
!
 dsl equipment-type CPE
```

```
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
!
connect frf5-v vc-group GroupA ATM0 0/33
```

Note For FRF.5, you may need to match the maximum transmission unit (MTU) between the ATM and Frame Relay networks for large size packets.

FRF.8 over G.SHDSL Example

The following output is from a Cisco 1721 router. This example shows how to create an FRF.8 connection using the the **connect** command with the **service-interworking** keyword.

```
frame-relay switching
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
!
interface ATM0.1 point-to-point
 pvc 0/33
  encapsulation aal5mux fr-atm-srv
!
interface Serial0
 no ip address
 encapsulation frame-relay IETF
 clockrate 2000000
 frame-relay interface-dlci 100 switched
 frame-relay intf-type dce
!
ip classless
no ip http server
!
connect frf8 Serial0 100 ATM0 0/33 service-interworking
```

Note For FRF.8, you may need to match the maximum transmission unit (MTU) between the ATM and Frame Relay networks for large size packets.

MLP Bundling Example

The following output examples show how MLP DSL links can be bundled using a multilink interface. The configurations were created using devices in a specific laboratory environment. All of the devices started with a cleared (default) configuration. If you are working in a live network situation, make sure that you understand the potential impact of all commands before using them (refer to the command references for Cisco IOS Release 12.2).

Note Before configuring MLP bundling, ensure that IP CEF is turned on for QoS.

The following example was configured on a Cisco 2600 router equipped with two xDSL WICs.

```
ip subnet-zero
ip cef
!
no ip domain lookup
!
class-map match-all VOICE
 match access-group 100
!
policy-map green
 class VOICE
  priority 100
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.0
!
interface Multilink1
 ip unnumbered Loopback0
 load-interval 30
 service-policy output green
  ip nat outside
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 6
 ppp multilink interleave
 multilink-group 1
!
interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0/0.1 point-to-point
 pvc 203/202
  vbr-rt 640 640
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface FastEthernet0/0
ip address 10.3.202.48 255.0.0.0
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
interface ATM0/1
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0/1.1 point-to-point
 pvc 5/201
  vbr-rt 640 640
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface FastEthernet0/1
 description ip address 10.6.6.6 255.0.0.0
 mac-address 0000.0000.0003
 ip address 10.1.1.30 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ppp authentication chap pap
```

```
 ppp multilink
 ppp multilink multiclass
 multilink-group 1
!
ip classless
ip route 10.1.1.0 255.255.255.0 2.2.2.3
ip route 10.1.1.1 255.255.255.255 2.2.2.3
ip route 192.168.254.254 255.255.255.255 1.3.0.1
no ip http server
ip pim bidir-enable
!
access-list 100 permit udp any any precedence critical
access-list 100 permit tcp any any eq 1720
access-list 100 permit tcp any eq 1720 any
no cdp run
!
snmp-server manager
call rsvp-sync
!
voice-port 1/1/0
!
voice-port 1/1/1
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 101 voip
 incoming called-number 10.....
 destination-pattern 200....
 session target ipv4:2.2.2.3
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 200 pots
 destination-pattern 100....
 port 1/1/0
 prefix 200
!
alias exec c conf t
alias exec s sh run
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 login
line vty 5 15
 login
```

The following example was configured on a Cisco 3660 or Cisco 7206 router:

```
ip subnet-zero
ip cef
!
no ip domain lookup
!
class-map match-all VOICE
 match access-group 100
!
policy-map PURPLE
 class VOICE
  priority 100
!
voice call carrier capacity active
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 10.2.2.3 255.255.255.0
```

```
!
interface Multilink1
 ip unnumbered Loopback0
 load-interval 30
 service-policy output PURPLE
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 6
 ppp multilink interleave
 multilink-group 1
!
interface FastEthernet0/0
 mac-address 0000.0000.0004
 ip address 10.3.202.89 255.0.0.0
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 mac-address 0000.0000.0004
 ip address 10.1.1.20 255.255.255.0
 load-interval 30
 no keepalive
 duplex auto
 speed auto
 no cdp enable
!
interface ATM2/0
 no ip address
 load-interval 30
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 pvc 203/202
  vbr-rt 640 640
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface ATM2/0.2 point-to-point
 pvc 5/201
  vbr-rt 640 640
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface Virtual-Template1
 no ip address
 load-interval 30
 ppp authentication chap pap
 ppp multilink
 ppp multilink multiclass
 multilink-group 1
!
ip classless
ip route 10.1.1.0 255.255.255.0 2.2.2.2
ip route 10.1.1.1 255.255.255.255 2.2.2.2
ip route 192.168.254.254 255.255.255.255 1.3.0.1
ip http server
ip pim bidir-enable
!
access-list 100 permit udp any any precedence critical
access-list 100 permit tcp any any eq 1720
access-list 100 permit tcp any eq 1720 any
no cdp run
!
call rsvp-sync
!
voice-port 4/1/0
!
voice-port 4/1/1
!
mgcp profile default
```

```
!
dial-peer cor custom
dial-peer voice 101 voip
 incoming called-number 200....
 destination-pattern 10.....
 session target ipv4:2.2.2.2
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
dial-peer voice 200 pots
 destination-pattern 200....
 port 4/1/0
 prefix 200
!
alias exec c conf t
alias exec s sh run
!
line con 0
 exec-timeout 0 0
 privilege level 15
 line aux 0
 line vty 0 4
 password green
 login
```

Tx Ring-Limit Tuning over ADSL Example

The following output is from a Cisco 1751 router. The tx ring limit is configured on an ATM PVC interface.

```
class-map match-all VOIP
 match ip dscp 32
class-map CRITICAL
 match access-group 100
!
policy-map 1751_ADSL
 class CRITICAL
  priority 48
 class VOIP
  bandwidth 64
  set ip precedence 6
!
interface Loopback1
ip address 10.0.0.10 255.255.255.252
!
interface ATM0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0/0.1
 pvc 0/33
  vbr-rt 320 320 30
  tx-ring-limit 3
  protocol ppp Virtual-Template1
!
interface Virtual-Template1
 bandwidth 320
 ip unnumbered Loopback1
 ip mroute-cache
 service-policy output 1751_ADSL
 ppp multilink
 ppp multilink fragment-delay 4
 ppp multilink interleave
```

The following output is from a Cisco 2600 router that is configured for tx ring-limit tuning:

```
voice-card 1
 dspfarm
!
```

```
ip subnet-zero
!
ip cef
!
class-map match-all VOICE-CLASS
 match access-group 100
!
policy-map SERVICE-PACK-640
 class VOICE-CLASS
  priority 160
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
 framing sf
 linecode ami
!
interface FastEthernet0/0
 ip address 10.3.214.50 255.255.0.0
 duplex auto
 speed auto
!
interface ATM0/1
 no ip address
 load-interval 30
 atm vc-per-vp 256
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
!
interface ATM0/1.1 point-to-point
 ip address 192.168.1.2 255.255.255.0
 pvc 11/201
  protocol ip 192.168.1.1 broadcast
  vbr-nrt 640 640
  tx-ring-limit 3
  oam-pvc manage
  service-policy output SERVICE-PACK-640
!
interface FastEthernet0/1
 ip address 10.10.11.1 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
!
ip classless
ip route 10.10.11.254 255.255.255.255 192.168.1.1
ip route 192.168.254.254 255.255.255.255 1.3.0.1
ip http server
ip pim bidir-enable
!
ip director cache time 60
access-list 100 permit udp any any precedence critical
!
snmp-server manager
call rsvp-sync
!
voice-port 1/0:0
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 1 pots
 destination-pattern 7...
!
dial-peer voice 2 voip
 pattern 8...
```

```
 session target ipv4:192.168.1.1
 ip qos dscp cs5 media
 ip qos dscp cs5 signaling
 no vad
!
alias exec s sh run
alias exec c conf t
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 login
line vty 5 15
 login
```

Additional References

Related Documents

Related Topic	Document Title
Configuring ATM	"Configuring ATM"
ATM commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples.	*Cisco IOS Asynchronous Transfer Mode Command Reference*
Configuring SNMP support	"Configuring SNMP Support"
SNMP commands	*Cisco IOS Network Management Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
• ATM PVC MIB • CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Asynchronous Transfer Mode Command Reference*. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List*.

- **clock rate** (interface ATM)
- **connect** (FRF.5)
- **connect** (FRF.8)
- **de-bit**
- **ppp multilink multiclass**
- **tx-ring-limit**

CHAPTER 14

End of Life for Multiprotocol over ATM

Support for Multiprotocol over ATM feature and commands has been removed in Cisco IOS Release 15.1M and later releases. This change marks the end of life for multiprotocol over ATM (MPOA).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Removal of Support for Multiprotocol over ATM

The following Multiprotocol over ATM feature is obsolete and is no longer available in Cisco IOS Release 15.1M and later releases:

- Multiprotocol over ATM Overview
- Configuring the Multiprotocol over ATM Server
- Configuring the Multiprotocol over ATM Client

Removal of Support for Multiprotocol over ATM Commands

The following commands are obsolete and are no longer available in Cisco IOS Release 15.1M and later releases (no replacement commands are provided):

- **debug mpoa client**
- **debug mpoa server**
- **mpoa client config name**
- **mpoa client name**
- **mpoa server config name**
- **mpoa server name**
- **mpoa server name trigger ip-address**
- **show mpoa client**
- **show mpoa client cache**
- **show mpoa client statistics**
- **show mpoa default-atm-addresses**
- **show mpoa server**
- **show mpoa server cache**
- **show mpoa server statistics**

Additional References

The following sections provide references related to the IEEE 802.1ah Support for Ethernet Infrastructure feature.

Related Documents

Related Topic	Document Title
Configuring ATM	Configuring ATM
ATM commands	Cisco IOS Asynchronous Transfer Mode Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for End of Life for Multiprotocol over ATM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 17: Feature Information for End of Life for Multiprotocol over ATM

Feature Name	Releases	Feature Information
End of Life for Multiprotocol over ATM	15.1M	Support for Multiprotocol over ATM has been removed from the Cisco IOS software.

CHAPTER 15

Multiprotocol over ATM Overview

This chapter describes the Multiprotocol over ATM (MPOA) feature, which is supported in Cisco IOS Release 11.3 and later releases.

MPOA enables the fast routing of internetwork-layer packets across a nonbroadcast multiaccess (NBMA) network. MPOA replaces multihop routing with point-to-point routing using a direct virtual channel connection (VCC) between ingress and egress edge devices or hosts. An ingress edge device or host is defined as the point at which an inbound flow enters the MPOA system; an egress edge device or host is defined as the point at which an outbound flow exits the MPOA system.

Procedures for configuring MPOA are provided in the following chapters in this publication:

- "Configuring the Multiprotocol over ATM Client" chapter
- "Configuring the Multiprotocol over ATM Server" chapter
- "Configuring Token Ring LAN Emulation for Multiprotocol over ATM" chapter

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Finding Feature Information

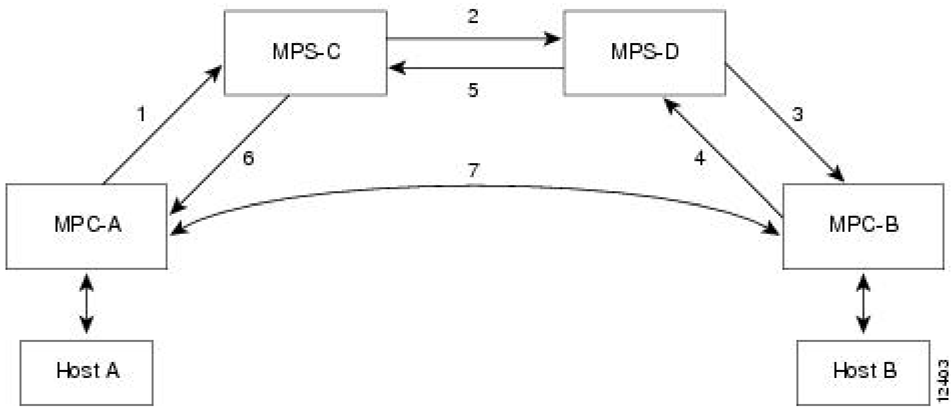
Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

How MPOA Works

In an NBMA network, intersubnet routing involves forwarding packets hop-by-hop through intermediate routers. MPOA can increase performance and reduce latencies by identifying the edge devices, establishing a direct VCC between the ingress and egress edge devices, and forwarding Layer 3 packets directly over this shortcut VCC, bypassing the intermediate routers. An MPOA client (MPC) provides the direct VCCs between the edge devices or hosts whenever possible and forwards Layer 3 packets over these shortcut VCCs. The MPCs must be used with MPSs resident on routers.

Figure 19: MPOA Message Flow Between MPCs and MPSs



The sequence of events shown in the figure are summarized as follows:

1. MPOA resolution request sent from MPC-A to MPS-C
2. NHRP resolution request sent from MPS-C to MPS-D
3. MPOA cache-imposition request sent from MPS-D to MPC-B
4. MPOA cache-imposition reply sent from MPC-B to MPS-D
5. NHRP resolution reply sent from MPS-D to MPS-C
6. MPOA resolution reply sent from MPS-C to MPC-A
7. Shortcut VCC established

The table below lists and defines the MPOA terms used in in the figure.

Table 18: MPOA Terms

MPOA Term	Definition
MPOA resolution request	A request from an MPC to resolve a destination protocol address to an ATM address to establish a shortcut VCC to the egress device.
NHRP resolution request	An MPOA resolution request that has been converted to an NHRP resolution request.

MPOA Term	Definition
MPOA cache-imposition request	A request from an egress MPS to an egress MPC providing the MAC rewrite information for a destination protocol address.
MPOA cache-imposition reply	A reply from an egress MPC acknowledging an MPOA cache-imposition request.
NHRP resolution reply	An NHRP resolution reply that eventually will be converted to an MPOA resolution reply.
MPOA resolution reply	A reply from the ingress MPS resolving a protocol address to an ATM address.
Shortcut VCC	The path between MPCs over which Layer 3 packets are sent.

Traffic Flow

The figure in the "How MPOA Works" section shows how MPOA messages flow from Host A to Host B. In this figure, an MPC (MPC-A) residing on a host or edge device detects a packet flow to a destination IP address (Host B) and sends an MPOA resolution request. An MPS (MPS-C) residing on a router converts the MPOA resolution request to an NHRP resolution request and passes it to the neighboring MPS/NHS (MPS-D) on the routed path. When the NHRP resolution request reaches the egress point, the MPS (MPS-D) on that router sends an MPOA cache-imposition request to MPC-B. MPC-B acknowledges the request with a cache-imposition reply and adds a tag that allows the originator of the MPOA resolution request to receive the ATM address of MPC-B. As a result, the shortcut VCC between the edge MPCs (MPC-A and MPC-B) is set up.

When traffic flows from Host A to Host B, MPC-A is the ingress MPC and MPC-B is the egress MPC. The ingress MPC contains a cache entry for Host B with the ATM address of the egress MPC. The ingress MPC switches packets destined to Host B on the shortcut VCC with the appropriate tag received in the MPOA resolution reply. Packets traversing through the shortcut VCC do not have any DLL headers. The egress MPC contains a cache entry that associates the IP address of Host B and the ATM address of the ingress MPC to a DLL header. When the egress MPC switches an IP packet through a shortcut path to Host B, it appears to have come from the egress router.

Interaction with LANE

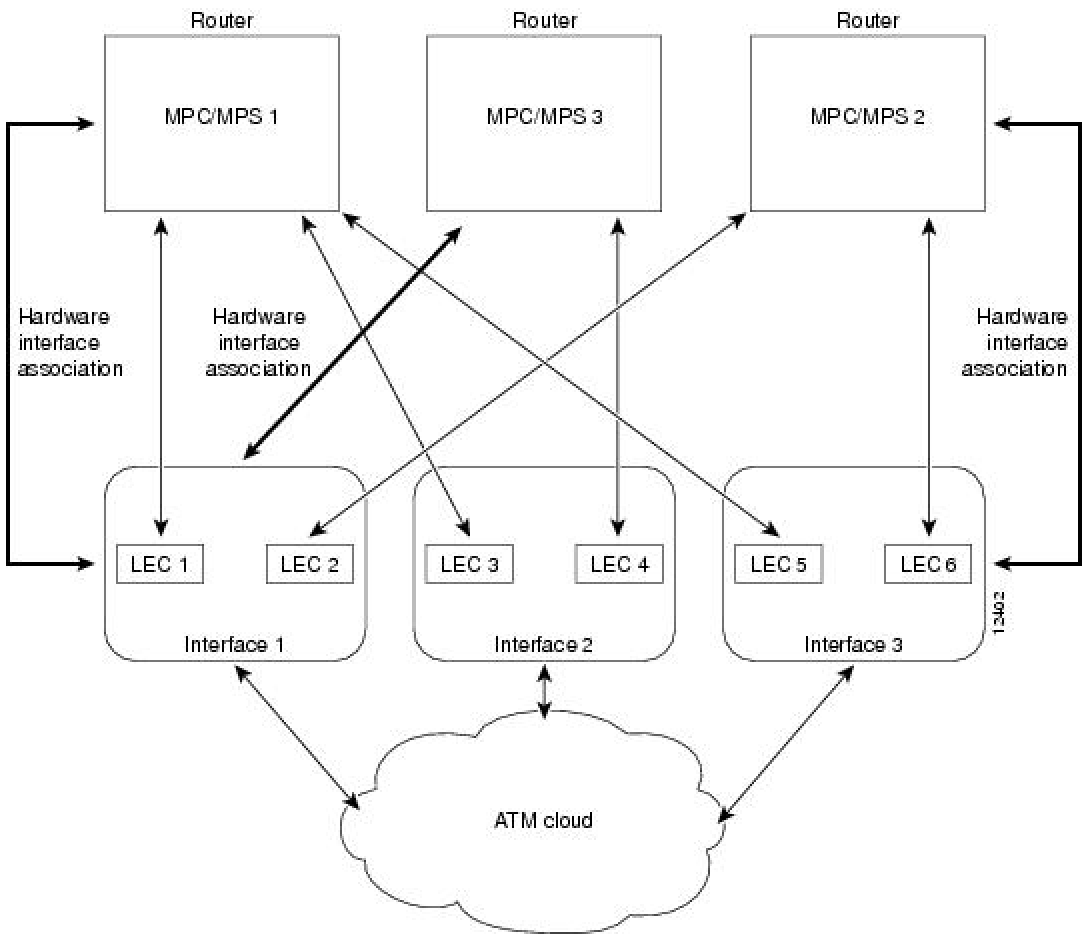
An MPOA functional network must have at least one MPS, one or more MPCs, and zero or more intermediate routers implementing NHRP servers. The MPSs and MPCs use LANE control frames to discover each other's presence in the LANE network.

Caution For MPOA to work properly, you must first create an ELAN identifier for each ELAN. Use the **lane config database** or the **lane server-bus** ATM LANE command to create ELAN identifiers. These commands are described in the *Catalyst 5000 Series Command Reference* publication.

An MPC/MPS can serve as one or more LAN Emulation Clients (LECs). The LEC can be associated with any MPC/MPS in the router or Catalyst 5000 series switch. A LEC can be attached both an MPC and an MPS simultaneously.

The figure below shows the relationships between MPC/MPS and LECs.

Figure 20: MPC-LEC and MPS-LEC Relationships



MPOA Components

The following components are required for an MPOA network:

- MPOA Client (MPC)
- MPOA Server (MPS)

- Catalyst 5000 series ATM module
- LAN Emulation (LANE)
- Next Hop Resolution Protocol (NHRP)

An MPC identifies packets sent to an MPS, establishes a shortcut VCC to the egress MPC, and then routes these packets directly over the shortcut VCC. An MPC can be a router or a Catalyst 5000 series ATM module. An MPS can be a router or a Catalyst 5000 series Route Switch Module/Versatile Interface Processor 2 (RSM/VIP2) with an ATM interface.

Note Since the RSM/VIP2 can also be used as a router, all references to *router* in this chapter refer to both a router and the RSM/VIP2 with an ATM interface.

Benefits

MPOA provides the following benefits:

- Eliminates multiple router hops between the source and the destination points of the ATM cloud by establishing shortcuts for IP packets and other protocol packets.
- Frees the router for other tasks by reducing IP traffic.
- Provides backward compatibility as an ATM network by building upon LANE, and can be implemented using both MPOA and LANE-only devices.

Configuring an MPC MPS

To configure an MPC/MPS, perform the following tasks:

- Define a name for the MPC/MPS.
- Attach the MPC/MPS to a major interface. This task serves two purposes:
    - Assigns an ATM address to the MPC/MPS.
    - Identifies an end point for initiating and terminating MPOA virtual circuits.
- Bind the MPC/MPS to multiple LECs.

Multiple MPCs/MPSs can run on the same physical interface, each corresponding to different control ATM address. Once an MPC/MPS is attached to a single interface for its control traffic, it cannot be attached to another interface unless you break the first attachment. The MPC/MPS is attached to subinterface 0 of the interface.

In the figure in the "Interaction with LANE" section, MPC/MPS 1 is attached to interface 1; MPC/MPS 1 can only use interface 1 to set up its control virtual circuits (VCs). MPC/MPS 2 is attached to interface 3; MPC/MPS 2 can only use interface 3 to set up its control VCs.

Note An MPC/MPS can be attached to a single hardware interface only.

More than one MPC/MPS can be attached to the same interface. MPC/MPS 3 and MPC/MPS 1 are both attached to interface 1, although they get different control addresses. Any LEC running on any subinterface of a hardware interface can be bound to any MPC/MPS. However, once a LEC is bound to a particular MPC/MPS, it cannot be bound to another MPC/MPS.

Note Once a LEC has been bound to an MPC/MPS, you must unbind the LEC from the first MPC/MPS before binding it to another MPC/MPS. Typically, you will not need to configure more than one MPS in a router.

Ensure that the hardware interface attached to an MPC/MPS is directly reachable through the ATM network by all the LECs that are bound to it.

Note If any of the LECs reside on a different (unreachable) ATM network from the one to which the hardware interface is connected, MPOA will not operate properly.

CHAPTER 16

Configuring the Multiprotocol over ATM Client

The Multiprotocol over ATM (MPOA) client (MPC) involves ingress/egress cache management, data-plane and control-plane virtual circuit connection (VCC) management, MPOA frame processing, and participation in MPOA protocol and MPOA flow detection.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the Multiprotocol over ATM Client

MPC Software Module

The MPC software module implements the functionality of the MPC in compliance with the ATM Forum MPOA specification. An MPC identifies packets sent to an MPOA-capable router over the nonbroadcast multi-access (NBMA) network and establishes a shortcut VCC to the egress MPC, if possible. The MPC then routes these packets directly over this shortcut VCC, bypassing the intermediate routers and enabling the fast routing of internetwork-layer packets across an NBMA network. The Catalyst 5000 series switch can be designated as an MPC. If the Catalyst 5000 series switch is configured with an RSM/VIP2 (with an ATM interface) it can be configured as an MPC or an MPS.

A router is usually designated as an MPOA server (MPS), but can also be designated as an MPC. MPC on the router is primarily meant to provide router-initiated and router-terminated shortcuts for non-NBMA networks. For this reason, MPC information in this chapter primarily refers to the Catalyst 5000 series switch, and MPS information refers to the router or the RSM/VIP2 with an ATM interface in a Catalyst 5000 series switch.

How to Configure the Multiprotocol over ATM Client

Configuring the ELAN ID

For MPOA to work properly, an LEC must belong to an ELAN that has a defined ELAN ID.

Caution If an ELAN ID is supplied, make sure both commands use the same elan-id value.

To obtain an ELAN ID, use either of the following commands in LANE database configuration mode.

Note To configure an MPC on a Catalyst 5000 series ATM module, establish a connection with the ATM module, enter privileged mode, and then enter configuration mode. For information on performing these tasks, refer to the *Catalyst 5000 Series Software Configuration Guide* .

Command or Action	Purpose
`Router(lane-config-dat)#` **name** *elan-name* **elan-id** *id*	Defines an ELAN ID for the LEC (in LANE database configuration mode).
`Router(lane-config-dat)#` **lane server-bus ethernet** *elan-name* [**elan-id** *id*]	Configures the LEC with the ELAN ID (in interface configuration mode).

Configuring the MPC

To configure an MPC on your network, perform the steps in this section.

SUMMARY STEPS

1. Router(config)# **mpoa client config name***mpc-name*
2. Router(config-if)# **interface atm** {*mod-num/port-num* | *number* }
3. Router(config-if)# **mpoa client name***mpc-name*
4. Router(config-if)# **interface***atm-num.sub-interface-num*
5. Router(config-if)# **lane client mpoa client name***mpc-name*
6. Repeat Steps 4 and 5 for every LEC to be served by the MPC/MPS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **mpoa client config name***mpc-name*	In global configuration mode, defines an MPC with a specified name.
Step 2	Router(config-if)# **interface atm** {*mod-num/port-num* | *number* }	In interface configuration mode, specifies the ATM interface to which the MPC is associated.
Step 3	Router(config-if)# **mpoa client name***mpc-name*	In interface configuration mode, attaches an MPC to the ATM interface.
Step 4	Router(config-if)# **interface***atm-num.sub-interface-num*	In interface configuration mode, specifies the ATM interface that contains the LEC to which you will bind the MPC.
Step 5	Router(config-if)# **lane client mpoa client name***mpc-name*	In interface configuration mode, binds a LEC to the specified MPC.
Step 6	Repeat Steps 4 and 5 for every LEC to be served by the MPC/MPS.	

Configuring the MPC Variables

An MPC has to be defined with a specified name before you can change its variables.

To change the variables for an MPC, perform the steps in this section.

SUMMARY STEPS

1. Router(mpoa-client-config)# **mpoa client config name***mps-name*
2. Router(mpoa-client-config)# **atm-address***atm-address*
3. Router(mpoa-client-config)# **shortcut-frame-count***count*
4. Router(mpoa-client-config)# **shortcut-frame-time***time*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(mpoa-client-config)# **mpoa client config name***mps-name*	Defines an MPC with the specified name.
Step 2	Router(mpoa-client-config)# **atm-address***atm-address*	(Optional) Specifies the control ATM address that the MPC should use (when it is associated with a hardware interface).
Step 3	Router(mpoa-client-config)# **shortcut-frame-count***count*	(Optional) Specifies the maximum number of times a packet can be routed to the default router within shortcut-frame time before an MPOA resolution request is sent.
Step 4	Router(mpoa-client-config)# **shortcut-frame-time***time*	(Optional) Sets the shortcut-setup frame time for the MPC.

Monitoring and Maintaining the MPC

To monitor and maintain the configuration of an MPC, use the following commands as needed.

SUMMARY STEPS

1. Router# **show mpoa client** [**name***mpc-name*]
2. Router# **show mpoa client** [**name***mpc-name*] **cache** [**ingress** | **egress**] [**ip-addr***ip-addr*]
3. Router# **show mpoa client** [**name***mpc-name*] **statistics**
4. Router# **clear mpoa client** [**name***mpc-name*] **cache** [**ingress** | **egress**] [**ip-addr***ip-addr*]
5. Router# **show mpoa client** [**name***mpc-name*] [*remote-device*]
6. Router# **show mpoa default-atm-addresses**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **show mpoa client** [**name***mpc-name*]	Displays information about a specified MPC or all MPCs.
Step 2	Router# **show mpoa client** [**name***mpc-name*] **cache** [**ingress**	**egress**] [**ip-addr***ip-addr*]	Displays ingress and egress cache entries associated with an MPC.
Step 3	Router# **show mpoa client** [**name***mpc-name*] **statistics**	Displays all the statistics collected by an MPC.
Step 4	Router# **clear mpoa client** [**name***mpc-name*] **cache** [**ingress**	**egress**] [**ip-addr***ip-addr*]	Clears cache entries.

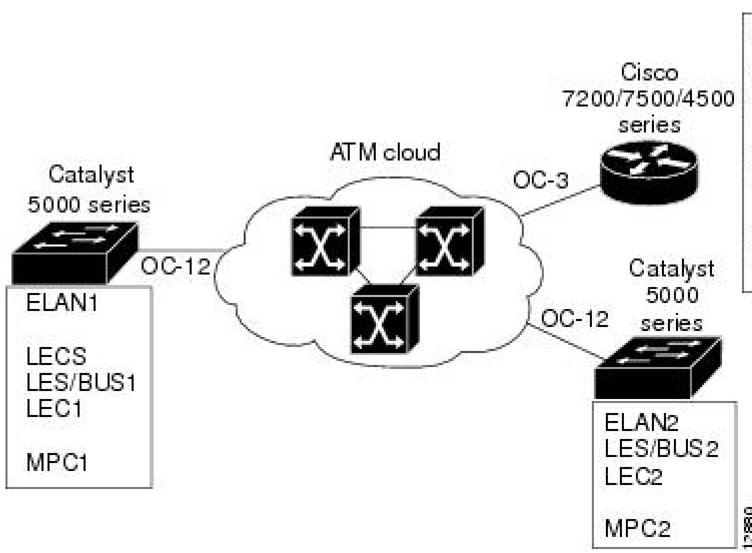
	Command or Action	Purpose
Step 5	Router# **show mpoa client** [**name***mpc-name*] [*remote-device*]	Displays all the MPOA devices that this MPC has learned.
Step 6	Router# **show mpoa default-atm-addresses**	Displays the default ATM addresses for the MPC.

Configuration Examples for the Multiprotocol over ATM Client

Configuring MCP Example

This section contains an example of the commands needed to configure an MPC. The lines beginning with exclamation points (!) are comments explaining the command shown on the subsequent line. The figure below shows an example of how you can configure your system to use MPOA.

Figure 21: Example of an MPOA Configuration



The following example shows how to configure the MPC and attach the MPC to a hardware interface:

```
! Define the MPC "MYMPC"
 mpoa client config name MYMPC
! Leave everything as default
 exit
! Specify the ATM interface to which the MPC is attached
 interface ATM 1/0
! Attach MPC MYMPC to the HW interface
 mpoa client name MYMPC
! Specify the ATM interface that contains the LEC to which you will bind the MPC
 interface atm 1/0.1
! Bind a LANE client to the specified MPC
 lane client mpoa client name MYMPC
```

```
! Go back up to global config mode
 exit
```

The following example shows a typical configuration file for the first MPC:

```
Current configuration:
!
version 11.3
! Go to LANE database config mode
 exit
lane database mpoa-test
hostname mpc-1
! Define the ELAN ID and ATM address
name elan1 server-atm-address 47.00918100000000613E5A2F01.006070174821.01
name elan1 elan-id 101
name elan2 server-atm-address 47.00918100000000613E5A2F01.006070174821.02
name elan2 elan-id 102
! Define the MPC "mpc-1"
mpoa client config name mpc-1
interface Ethernet0
! Go back up to global config mode
 exit
! Specify the ATM interface to which the MPC is attached
interface ATM0
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
lane config auto-config-atm-address
lane config database mpoa-test
! Attach MPC mpc-1 to the HW interface
mpoa client name mpc-1
! Specify the ATM interface that contains the LEC to which you will bind the MPC
interface ATM0.1 multipoint
lane server-bus ethernet elan1
! Bind a LANE client to the specified MPC
lane client mpoa client name mpc-1
lane client ethernet 1 elan1
! Go back up to global config mode
 exit
```

The following example shows a typical configuration file for the second MPC:

```
Current configuration:
!
version 11.3
hostname mpc-2
! Go back up to global config mode
 exit
! Define the MPC "mpc-2"
mpoa client config name mpc-2
! Specify the ATM interface to which the MPC is attached
interface ATM0
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
mpoa client name mpc-2
! Specify the ATM interface that contains the LEC to which you will bind the MPC
interface ATM0.1 multipoint
lane server-bus ethernet elan2
lane client mpoa client name mpc-2
lane client ethernet 2 elan2
! Go back up to global config mode
 exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*

Standards

Standard	Title
None	

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the Multiprotocol over ATM Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 19: Feature Information for the Multiprotocol over ATM Client

Feature Name	Releases	Feature Information
Multiprotocol over ATM Client	12.0(1) 12.1(1)E	The Multiprotocol over ATM (MPOA) client (MPC) involves ingress/egress cache management, data-plane and control-plane virtual circuit connection (VCC) management, MPOA frame processing, and participation in MPOA protocol and MPOA flow detection. The following commands were introduced or modifief: **clear mpoa client cache**, **debug mpoa client**, **lane client mpoa client name**, **mpoa client config name**, **mpoa client name**, **show mpoa client**, **show mpoa client cache**, **show mpoa client statistics**.

CHAPTER 17

Configuring the Multiprotocol over ATM Server

The Multiprotocol over ATM (MPOA) server (MPS) supplies the forwarding information used by the MPOA clients (MPCs). The MPS responds with the information after receiving a query from a client. To support the query and response functions, MPOA has adopted the Next Hop Resolution Protocol (NHRP). The MPS on the router can also terminate shortcuts.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

How MPS Works

The MPS software module implements the functionality of the MPS in compliance with the ATM Forum MPOA specification. The following sections describe the functions of MPS:

MPS-NHRP-Routing Interaction

MPS must interact with the NHRP module in the router to smoothly propagate MPOA/NHRP packets end to end. MPOA frames are identical to NHRP frames except for some specific op-codes and extensions for MPOA.

The following process explains the interaction of MPS and NHRP:

1. MPS converts MPOA resolution requests to NHRP requests and sends it either to the next hop MPS or to the Next Hop Server (NHS), depending on the configuration. MPS searches for the next hop routing information to determine the interface and sends the packet with correct encapsulation to an MPS or an NHS.
2. NHS sends resolution requests to MPS when the next hop is on a LAN Emulation (LANE) cloud or when NHS is unsure of the packet destination. MPS may do further processing, such as prompt NHS to terminate the request or throw away the packet.
3. NHS sends resolution replies to MPS when the next hop interface is LANE or when the replies terminate in the router. Then MPS sends an MPOA resolution reply to the MPC.

Shortcut Domains

Within a router, it is possible to permit shortcuts between one group of LAN Emulation Clients (LECs) and deny it between some other groups of LECs. Cisco introduces a notion of network ID associated with an MPS. By default, all the MPSs in a router get a network ID of 1.

If the administrator wants to segregate traffic, then MPSs can be given different network IDs, in effect preventing shortcuts between LECs served by different MPSs. This can be configured in the definition of an MPS database.

If a router has both MPS and NHRP configured, then the same network ID is required to facilitate requests, replies, and shortcuts across the MPS and NHRP. The interface-specific NHRP command (**ip nhrp network-id**) must be the same for an MPS; otherwise, there will be a disjointed network.

MPS Configuration Task List

Configuring the ELAN ID

For MPOA to work properly, a LANE client must have an ELAN ID for all ELANs represented by the LANE clients.

Caution If an ELAN ID is supplied by both commands, make sure that the ELAN ID matches in both.

To configure an ELAN ID, use either of the following commands in lane database configuration mode or in interface configuration mode when starting up the LAN Emulation Client Server (LECS) for that ELAN:

Command	Purpose
Router(lane-config-dat)# **name** *elan-name* **elan-id** *id*	Configures the ELAN ID in the LECS database to participate in MPOA.
Router(lane-config-dat)# **lane server-bus** {**ethernet** | **tokenring**} *elan-name* [**elan-id** *id*]	Configures the LAN Emulation Server (LES) with the ELAN ID to participate in MPOA.

Configuring the MPS

To configure an MPS, use the following commands beginning in global configuration mode. The MPS starts functioning only after it is attached to a specific hardware interface:

SUMMARY STEPS

1. Router(config)# **mpoa server config name***mps-name*
2. Router(config)# **interface atm** {*slot/port* \| *number* }
3. Router(config-if)# **mpoa server name***mps-name*
4. Router(config-if)# **interface atm** {*slot/port.subinterface-number* \| *number***.***subinterface-number* }
5. Router(config-subif)# **lane client mpoa server name***mps-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **mpoa server config name***mps-name*	In global configuration mode, defines an MPS with the specified name.
Step 2	Router(config)# **interface atm** {*slot/port* | *number* }	Specifies the ATM interface to attach the MPS.
Step 3	Router(config-if)# **mpoa server name***mps-name*	In interface configuration mode, attaches the MPS to the ATM interface.
Step 4	Router(config-if)# **interface atm** {*slot/port.subinterface-number* | *number***.***subinterface-number* }	Specifies the ATM interface to bind the MPS to a LEC.
Step 5	Router(config-subif)# **lane client mpoa server name***mps-name*	In subinterface configuration mode, binds a LANE client to the specified MPS.

Configuring the MPS Variables

An MPS must be defined with a specified name before you can change the MPS variables specific to that MPS.

To change MPS variables specific only to a particular MPS, use the following commands beginning in MPS configuration mode:

SUMMARY STEPS

1. Router(mpoa-server-config)# **mpoa server config name***mps-name*
2. Router(mpoa-server-config)# **atm-address***atm-address*
3. Router(mpoa-server-config)# **holding-time***time*
4. Router(mpoa-server-config)# **keepalive-lifetime***time*
5. Router(mpoa-server-config)# **keepalive-time***time*
6. Router(mpoa-server-config)# **network-id***id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(mpoa-server-config)# **mpoa server config name***mps-name*	Defines an MPS with the specified name.
Step 2	Router(mpoa-server-config)# **atm-address***atm-address*	(Optional) Specifies the control ATM address that the MPS should use (when it is associated with a hardware interface).
Step 3	Router(mpoa-server-config)# **holding-time***time*	(Optional) Specifies the holding time value for the MPS-p7 variable of the MPS.
Step 4	Router(mpoa-server-config)# **keepalive-lifetime***time*	(Optional) Specifies the keepalive lifetime value for the MPS-p2 variable of the MPS.
Step 5	Router(mpoa-server-config)# **keepalive-time***time*	(Optional) Specifies the keepalive time value for the MPS-p1 variable of the MPS.
Step 6	Router(mpoa-server-config)# **network-id***id*	(Optional) Specifies the network ID of the MPS.

Monitoring and Maintaining the MPS

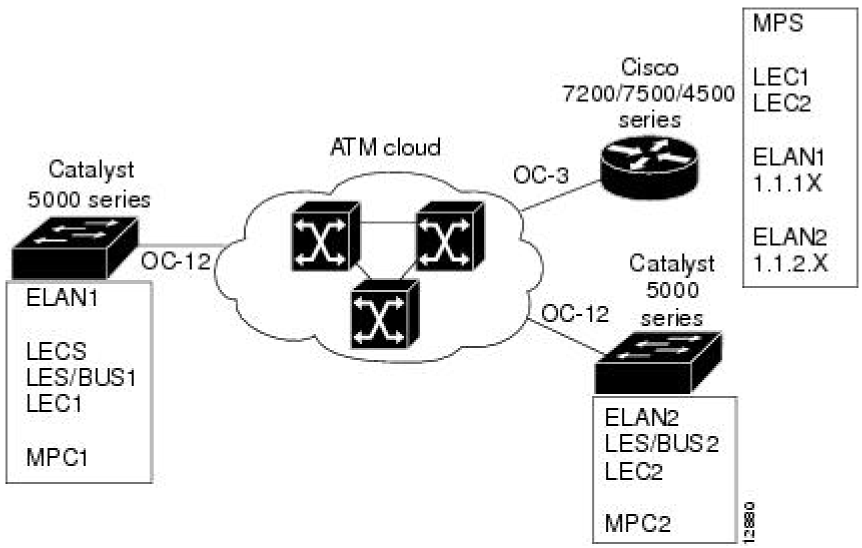
To monitor and maintain the configuration of an MPS, use the following commands in EXEC mode, as needef:

Command	Purpose
Router# **show mpoa default-atm-addresses**	Displays default ATM addresses for an MPS.
Router# **show mpoa server** [**name** *mps-name*]	Displays information about a specified server or all servers depending on the specified name of the required server.
Router# **show mpoa server** [**name** *mps-name*] **cache** [**ingress** | **egress**] [**ip-address** *ip-address*]	Displays ingress and egress cache entries associated with a server.
Router# **show mpoa server** [**name** *mps-name*] **statistics**	Displays all the statistics collected by a server including the ingress and egress cache entry creations, deletions, and failures.
Router# **clear mpoa server** [**name** *mps-name*] **cache** [**ingress** | **egress**] [**ip-addr** *ip-addr*]	Clears cache entries.
Router# **mpoa server name** *mps-name* **trigger ip-address** *ip-address* [**mpc-address** *mpc-address*]	Originates an MPOA trigger for the specified IP address to the specified client. If a client is not specified, the MPOA is triggered to all the clients.

MPS Configuration Example

This section contains an example of the commands needed to configure an MPS. The lines beginning with exclamation points (!) are comments explaining the command shown on the following line. The figure below shows an example of how you can configure your system to utilize MPOA.

Figure 22: Example of an MPOA Configuration



The following example configures the MPS and attaches the MPS to a hardware interface:

```
! Define the MPS "MYMPS"
 mpoa server config name MYMPS
! Leave everything as default
 exit
! Enter into interface config mode
 interface ATM 1/0
! Attach MPS MYMPS to the HW interface
 mpoa server name MYMPS
! Go back up to global config mode
 exit
```

The following example shows a typical MPS configuration file:

```
version 11.3
hostname MPS
! Define the MPS "mps"
mpoa server config name mps
! Specify the ATM interface to which the MPS is attached
interface ATM4/0
no ip address
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
lane config auto-config-atm-address
mpoa server name mps
! Specify the ATM interface that contains the LEC to which you will bind the MPS
interface ATM4/0.1 multipoint
ip address 1.1.1.2 255.255.255.0
lane client mpoa server name mps
lane client ethernet elan1
interface ATM4/0.2 multipoint
ip address 1.1.2.1 255.255.255.0
```

```
lane client mpoa server name mps
lane client ethernet elan2
end
```

Feature Information for the Multiprotocol over ATM Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 20: Feature Information for the Multiprotocol over ATM Client

Feature Name	Releases	Feature Information
Multiprotocol over ATM Server	12.0(1) 12.1(1)E	The Multiprotocol over ATM (MPOA) server (MPS) supplies the forwarding information used by the MPOA clients (MPCs). The MPS responds with the information after receiving a query from a client. To support the query and response functions, MPOA has adopted the Next Hop Resolution Protocol (NHRP). The MPS on the router can also terminate shortcuts. The following commands were introduced or modifief: **clear mpoa server cache**, **debug mpoa server**, **lane client mpoa server name**, **mpoa server config name**, **mpoa server name**, **show mpoa server**, **show mpoa server cache**, **show mpoa server statistics**.

CHAPTER 18

Configuring Token Ring LAN Emulation MPOA

This chapter describes the required and optional tasks for configuring the Multiprotocol over ATM (MPOA) for Token Ring Networks feature.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

The MPOA for Token Ring Networks feature allows Token Ring hosts on an ATM network to communicate over direct paths (called shortcuts) through the ATM network. These shortcuts bypass the intermediate router hops that otherwise would be encountered in the default path.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

How Token Ring MPOA Works

Token Ring Multiprotocol over ATM (MPOA) is an extension to LAN Emulation (LANE). It allows Token Ring LANE clients to forward IP packets between subnets to other Token Ring LANE clients through a shortcut in the ATM network. The Token Ring LANE clients have an MPOA client (MPC) communicating with an MPOA server (MPS) to establish this shortcut.

Token Ring LANE for MPOA Configuration Task List

Configuring a Token Ring LEC

For MPOA operation, a LEC must be associated with an MPS, an MPC, or both. Once a LEC is bound to a particular MPS/MPC, it cannot be bound to another MPS/MPC at the same time.

The LEC must also be associated with a physical interface or subinterface, which may be different from the physical interface associated with the MPS or MPC. For proper operation, all interfaces must belong to the same ATM network.

To configure a Token Ring LEC, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** {*slot*/*port*.*subinterface-number* | *number*.*subinterface-number* }
2. Router(config-if)# **lane client tokenring** [*elan-name*]
3. Router(config-if)# **lane client mpoa server***mps-name*
4. Router(config-if)# **lane client mpoa client***mpc-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** {*slot*/*port*.*subinterface-number* | *number*.*subinterface-number* }	Specifies the ATM interface to be associated with the LEC.
Step 2	Router(config-if)# **lane client tokenring** [*elan-name*]	Defines a Token Ring LEC on a specified ELAN name.
Step 3	Router(config-if)# **lane client mpoa server***mps-name*	(Optional) Binds a Token Ring LEC to an MPS.
Step 4	Router(config-if)# **lane client mpoa client***mpc-name*	(Optional) Binds a Token Ring LEC to an MPC.

Configuring the LECS Database

To configure the LECS database, use the following commands in beginning global configuration mode:

SUMMARY STEPS

1. Router(config)# **lane database***database-name*
2. Router(lane-config-dat)# **name***elan-name***server-atm-address***atm-address*
3. Router(lane-config-dat)# **name***elan-name***elan-id***id*
4. Router(lane-config-dat)# **name***elan-name* **local-seg-id***id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **lane database***database-name*	Creates a named database for the LECS.
Step 2	Router(lane-config-dat)# **name***elan-name***server-atm-address***atm-address*	Binds the name of the ELAN to the ATM address of the LES.
Step 3	Router(lane-config-dat)# **name***elan-name***elan-id***id*	Defines the ELAN ID in the LECS database to participate in MPOA.
Step 4	Router(lane-config-dat)# **name***elan-name* **local-seg-id***id*	Configures the local segment ID number.

Configuring the LES BUS

To configure the LES/BUS, use the following commands in beginning global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** {*slot*/*port*.*subinterface-number* | *number*.*subinterface-number* }
2. Router(config-if)# **lane server-bus tokenring***elan-name* [**elan-id***elan-id*]

DETAILED STEPS

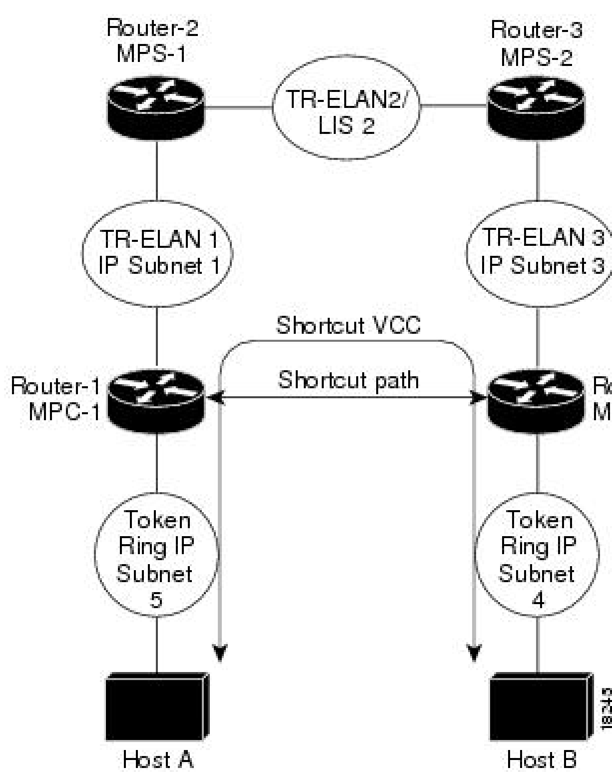
	Command or Action	Purpose
Step 1	Router(config)# **interface atm** {*slot*/*port*.*subinterface-number* | *number*.*subinterface-number* }	Specifies the ATM subinterface to be associated with the LES/BUS.
Step 2	Router(config-if)# **lane server-bus tokenring***elan-name* [**elan-id***elan-id*]	Defines a Token Ring LES/BUS on the named ELAN. The ELAN ID is optional.

Token Ring LANE Configuration Examples

MPOA Token Ring LANE Configuration in an IP-Routed Domain Example

The figure below illustrates MPOA in a Token Ring LANE environment where MPC-to-MPC shortcuts are established between Token Ring LANE edge routers that reside in different IP-routed domains.

Figure 23: Token Ring MPOA--MPC to MPC Shortcut in an IP Routed Environment



The following commands show a sample configuration for Router-1 in the figure:

```
hostname Router-1
!
ip routing
!
! Define the MPOA Client (mpc-1) configuration.
!
mpoa client config name mpc-1
!
! Configure an IP address on the Token Ring interface.
!
interface TokenRing1/0
 ip address 5.5.5.2 255.255.255.0
 ring-speed 16
!
```

```
! Configure a config-server and bind it to its database (mpoa-db).
! Attach the MPOA client mpc-1 to its ATM interface.
!
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database mpoa-db
 mpoa client name mpc-1
!
! Configure a LANE server-bus and LANE client on ELAN 1. Bind the
! LANE client to its MPOA Client (mpc-1).
!
interface ATM2/0.1 multipoint
 ip address 1.1.1.1 255.255.255.0
 lane server-bus tokenring 1
 lane client mpoa client name mpc-1
 lane client tokenring 1
!
router eigrp 1
 network 1.0.0.0
 network 5.0.0.0
!
end
```

The following commands show a sample configuration for Router-2 in the figure:

```
hostname Router-2
!
ip routing
!
! Configure the config-server database mpoa-db with configuration
! for ELANs 1 to 3
!
lane database mpoa-db
 name 1 server-atm-address 47.00918100000000060705BFA01.00000CA05F41.01
 name 1 local-seg-id 1000
 name 1 elan-id 100
 name 2 server-atm-address 47.00918100000000060705BFA01.00000CA05B41.01
 name 2 local-seg-id 2000
 name 2 elan-id 200
 name 3 server-atm-address 47.00918100000000060705BFA01.00000CA05B41.03
 name 3 local-seg-id 3000
 name 3 elan-id 300
!
! Define the MPOA Server (mps-1) configuration.
mpoa server config name mps-1
!
! Configure the signalling and ILMI PVCs. Also configure a config-server
! and attach the MPOA server (mps-1) to its ATM interface.
!
interface ATM4/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database mpoa-db
 mpoa server name mps-1
!
! Configure a Token Ring LANE client on ELAN 1 and bind the LANE
! client to its MPOA server (mps-1).
!
interface ATM4/0.1 multipoint
 ip address 1.1.1.2 255.255.255.0
 lane client mpoa server name mps-1
 lane client tokenring 1
!
! Configure a Token Ring LANE client on ELAN 2 and bind the LANE
! client to its MPOA server (mps-1)
!
interface ATM4/0.2 multipoint
 ip address 2.2.2.1 255.255.255.0
```

```
 lane client mpoa server name mps-1
 lane client tokenring 2
!
router eigrp 1
 network 1.0.0.0
 network 2.0.0.0
!
end
```

The following commands show a sample configuration for Router-3 in the figure:

```
hostname Router-3
!
ip routing
!
! Defines the MPOA Server (mps-2) configuration.
mpoa server config name mps-2
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! server (mps-2) to its ATM interface.
!
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 mpoa server name mps-2
!
! Configure a Token Ring LANE client and LANE server-bus on ELAN 2
! and bind the LANE client to its MPOA server (mps-2)
!
interface ATM2/0.1 multipoint
 ip address 2.2.2.2 255.255.255.0
 lane server-bus tokenring 2
 lane client mpoa server name mps-2
 lane client tokenring 2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA server (mps-2)
!
interface ATM2/0.3 multipoint
 ip address 3.3.3.1 255.255.255.0
 lane server-bus tokenring 3
 lane client mpoa server name mps-2
 lane client tokenring 3
!
router eigrp 1
 network 2.0.0.0
 network 3.0.0.0
!
end
```

The following commands show a sample configuration for Router-4 in the figure:

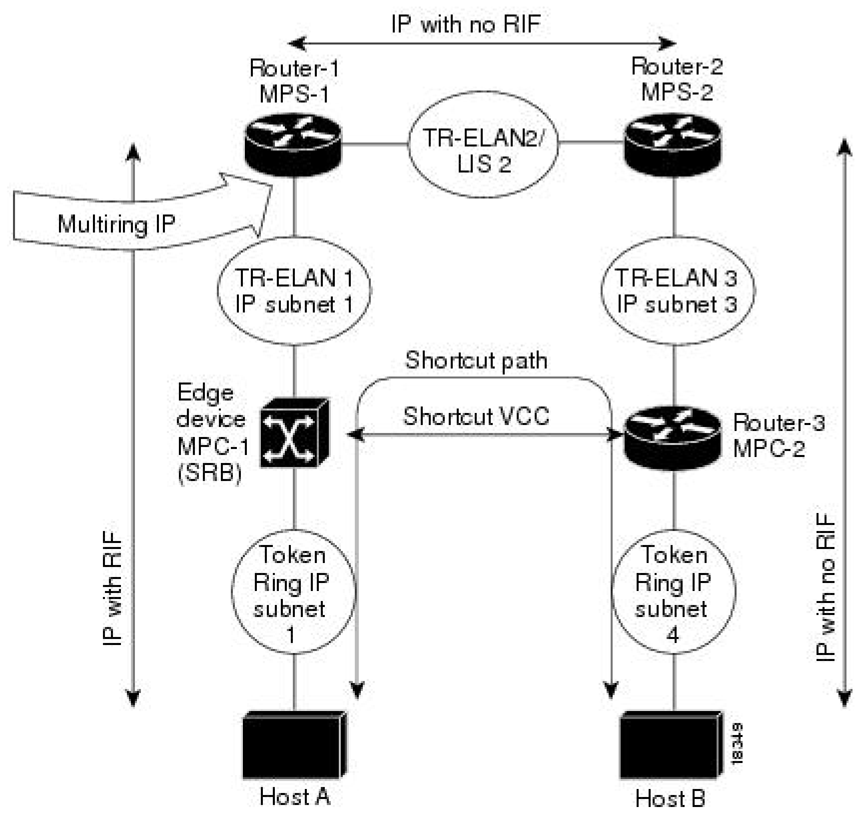
```
hostname Router-4
!
ip routing
!
! Define the MPOA client (mpc-2) configuration.
!
mpoa client config name mpc-2
!
! Configure the Token Ring interface
!
interface TokenRing1/0
 ip address 4.4.4.1 255.255.255.0
 ring-speed 16
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! client to its ATM interface.
!
interface ATM2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
```

```
 mpoa client name mpc-2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA client (mpc-2).
!
interface ATM2/0.1 multipoint
 ip address 3.3.3.2 255.255.255.0
 lane client mpoa client name mpc-2
 lane client tokenring 3
!
router eigrp 1
 network 3.0.0.0
 network 4.0.0.0
!
end
```

MPOA Token Ring LANE Configuration in an IP SRB-Routed Domain Example

The figure below illustrates MPOA in a Token Ring LANE environment where MPC-to-MPC shortcuts are established between a Token Ring LANE edge device and a Token Ring LANE router that reside in an IP SRB domain and IP-routed domains.

Figure 24: Token Ring MPOA--MPC to MPC Shortcut in an IP SRB-Routed Environment



The following commands show a sample configuration for Router-1 in the figure:

```
hostname Router-1
!
ip routing
```

```
!
! Configure the config-server database mpoa-db with configuration
! for ELANs 1 to 3
lane database mpoa-db
  name 1 server-atm-address 47.0091810000000060705BFA01.00000CA05F41.01
  name 1 local-seg-id 1000
  name 1 elan-id 100
  name 2 server-atm-address 47.0091810000000060705BFA01.00000CA05B41.01
  name 2 local-seg-id 2000
  name 2 elan-id 200
  name 3 server-atm-address 47.0091810000000060705BFA01.00000CA05B41.03
  name 3 local-seg-id 3000
  name 3 elan-id 300
!
! Define the MPOA Server (mps-1) configuration.
mpoa server config name mps-1
!
! Configure the signalling and ILMI PVCs. Also configure a config-server
! and attach the MPOA server (mps-1) to its ATM interface.
interface ATM4/0
  no ip address
  atm pvc 1 0 5 qsaal
  atm pvc 2 0 16 ilmi
  lane config auto-config-atm-address
  lane config database mpoa-db
  mpoa server name mps-1
!
! Configure a Token Ring LANE client on ELAN 1 and bind the LANE
! client to its MPOA server (mps-1). The multiring ip configuration
! is required to terminate the RIF for IP packets on the ELAN.
interface ATM4/0.1 multipoint
  ip address 1.1.1.2 255.255.255.0
  lane client mpoa server name mps-1
  lane client tokenring 1
  multiring ip
!
! Configure a Token Ring LANE client on ELAN 2 and bind the LANE
! client to its MPOA server (mps-1)
!
 interface ATM4/0.2 multipoint
   ip address 2.2.2.1 255.255.255.0
   lane client mpoa server name mps-1
   lane client tokenring 2
!
!
 router eigrp 1
   network 1.0.0.0
   network 2.0.0.0
!
end
```

The following commands show a sample configuration for Router-2 in the figure:

```
hostname Router-2
!
ip routing
!
! Defines the MPOA Server (mps-2) configuration.
mpoa server config name mps-2
!
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! server (mps-2) to its ATM interface.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 mpoa server name mps-2
!
! Configure a Token Ring LANE client and LANE server-bus on ELAN 2
! and bind the LANE client to its MPOA server (mps-2)
!
interface ATM2/0.1 multipoint
```

```
 ip address 2.2.2.2 255.255.255.0
 lane server-bus tokenring 2
 lane client mpoa server name mps-2
 lane client tokenring 2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA server (mps-2)
!
interface ATM2/0.3 multipoint
 ip address 3.3.3.1 255.255.255.0
 lane server-bus tokenring 3
 lane client mpoa server name mps-2
 lane client tokenring 3
!
router eigrp 1
 network 2.0.0.0
 network 3.0.0.0
!
end
```

The following commands show a sample configuration for Router-3 in the figure:

```
hostname Router-3
!
ip routing
!
! Define the MPOA client (mpc-2) configuration.
mpoa client config name mpc-2
!
!
! Configure the Token Ring interface
interface TokenRing1/0
 ip address 4.4.4.1 255.255.255.0
 ring-speed 16
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! client to its ATM interface.
!
interface ATM2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 mpoa client name mpc-2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA client (mpc-2).
!
interface ATM2/0.1 multipoint
 ip address 3.3.3.2 255.255.255.0
 lane client mpoa client name mpc-2
 lane client tokenring 3
!
router eigrp 1
 network 3.0.0.0
 network 4.0.0.0
!
end
```

CHAPTER 19

MPLS Diff-Serv-aware Traffic Engineering over ATM

This guide presents extensions made to Multiprotocol Label Switching Traffic Engineering (MPLS TE) that make it Diff-Serv aware and applicable across ATM networks. The bandwidth reservable on each link for constraint-based routing (CBR) purposes can now be managed through two bandwidth pools: a *global pool* and a *sub-pool*. The sub-pool can be limited to a smaller portion of the link bandwidth. Tunnels using the sub-pool bandwidth can then be used in conjunction with MPLS Quality of Service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network.

Caution The Fast Reroute feature of traffic engineering is not supported on ATM interfaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature History

Release	Modification
12.0(11) ST	DS-TE feature introduced.
12.0(14) ST	Support added for IS-IS Interior Gateway Protocol.
12.0(14) ST-1	Support added for guaranteed bandwidth service directed to many destination prefixes (for example, guaranteed bandwidth service destined to an autonomous system or to a BGP community).
12.2(4) T	Support added for Cisco Series 7200 platform and for ATM-PVC interface.
12.2(8) T	Support added for LC-ATM interface.

Background and Overview

MPLS traffic engineering allows constraint-based routing of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Diff-Serv-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of "guaranteed" traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a *sub-pool*, while the regular TE tunnel bandwidth is called the *global pool*. (The sub-pool is a portion of the global pool.) This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

For example, DS-TE can be used to ensure that traffic is routed over the network so that, on every link, there is never more than 40 per cent (or any assigned percentage) of the link capacity of guaranteed traffic (for example, voice), while there can be up to 100 per cent of the link capacity of regular traffic. Assuming QoS mechanisms are also used on every link to queue guaranteed traffic separately from regular traffic, it then becomes possible to enforce separate "overbooking" ratios for guaranteed and regular traffic. (In fact, for the guaranteed traffic it becomes possible to enforce no overbooking at all--or even an underbooking--so that very high QoS can be achieved end-to-end for that traffic, even while for the regular traffic a significant overbooking continues to be enforced.)

Also, through the ability to enforce a maximum percentage of guaranteed traffic on any link, the network administrator can directly control the end-to-end QoS performance parameters without having to rely on over-engineering or on expected shortest path routing behavior. This is essential for transport of applications that have very high QoS requirements (such as real-time voice, virtual IP leased line, and bandwidth trading), where over-engineering cannot be assumed everywhere in the network.

DS-TE involves extending OSPF (Open Shortest Path First routing protocol), so that the available sub-pool bandwidth at each preemption level is advertised in addition to the available global pool bandwidth at each preemption level. And DS-TE modifies constraint-based routing to take this more complex advertised information into account during path computation.

Benefits

Diff-Serv-aware Traffic Engineering enables service providers to perform separate admission control and separate route computation for discrete subsets of traffic (for example, voice and data traffic).

Therefore, by combining DS-TE with other IOS features such as QoS, the service provider can:

- Develop QoS services for end customers based on *signaled* rather than *provisioned* QoS
- Build the higher-revenue generating "strict-commitment" QoS services, without over-provisioning
- Offer virtual IP leased-line, Layer 2 service emulation, and point-to-point guaranteed bandwidth services including voice-trunking
- Enjoy the scalability properties offered by MPLS

Related Features and Technologies

The DS-TE feature is related to OSPF, IS-IS, RSVP (Resource reSerVation Protocol), QoS, and MPLS traffic engineering. Cisco documentation for all of these features is listed in the next section.

Related Documents

For OSPF:

- "Configuring OSPF" in Cisco IOS Release 12.1 *IP and IP Routing Configuration Guide*.
- "OSPF Commands" in Cisco IOS Release 12.1 IP and *IP Routing Command Reference*.

For IS-IS:

- "Configuring Integrated IS-IS" in Cisco IOS Release 12.1 *IP and IP Routing Configuration Guide*.
- "Integrated IS-IS Commands" in Cisco IOS Release 12.1 *Cisco IOS IP and IP Routing Command Reference*.

For RSVP:

- "Configuring RSVP" in Cisco IOS Release 12.1 *Quality of Service Solutions Configuration Guide*.
- IP RSVP commands section in Cisco IOS Release 12.1 *Quality of Service Solutions Command Reference*.

For QoS:

- Cisco IOS Release 12.1 *Quality of Service Solutions Configuration Guide*.
- Cisco IOS Release 12.1 *Quality of Service Solutions Command Reference*.

For MPLS Traffic Engineering:

- Cisco IOS Release 12.1(3)T *MPLS Traffic Engineering and Enhancements*
- "Multiprotocol Label Switching" in Cisco IOS Release 12.1 *Switching Services Configuration Guide*.
- Section containing MPLS commands in Cisco IOS Release 12.1 *Switching Services Command Reference*.

For ATM:

- ATM-PVC: the "Configuring ATM" chapter of the Release 12.2 *Cisco IOS Wide-Area Networking Configuration Guide*.
- ATM-LSR: the "Configuring Trunks and Adding Interface Shelves" chapter of the Release 9.3.30 *BPX 8600 Series Installation and Configuration Guide* http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/9_3_3/iandc/bpxi18.htm and the Release 9.3.10 *Update to the Cisco WAN Switch Command Reference Guide* http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/9_3_1/update/udcmdref.htm

Platforms and Interfaces Supported

This release supports DS-TE together with QoS on the POS, ATM-PVC, and LC-ATM interfaces of the Cisco 7200 and 7500 Series Routers.

To carry DS-TE tunnels through an MPLS ATM cloud, an ATM-LSR should contain a Cisco 7200 router (functioning as its Label Switch Controller) and any one of the following ATM switches:

- Cisco BPX 8600, 8650, or 8680
- Cisco IGX 8410, 8420, or 8430

To check for changes in platform support since the publication of this document, access *Feature Navigator* at http://www.cisco.com/go/fn . You must have an account on Cisco.com . Qualified users can establish an account by following directions at http://www.cisco.com/register .

If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered, and account details with a new random password will then be e-mailed to you.

Supported Standards

Standardization of Diff-Serv-aware MPLS Traffic Engineering is still in progress in the IETF (Internet Engineering Task Force). At the time of publication of this feature guide, DS-TE has been documented in the following IETF drafts:

- *Requirements for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, A. Chiu, W. Townsend, D. Skalecki & M. Tatham*http://search.ietf.org/internet-drafts/draft-ietf-tewg-diff-te-reqts-nn.txt*
- *Protocol Extensions for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, J. Boyle, K. Kompella, W. Townsend & D. Skalecki*http://search.ietf.org/internet-drafts/draft-ietf-tewg-diff-te-proto-01.txt*

As the IETF work is still in progress, details are still under definition and subject to change, so DS-TE should be considered as a pre-standard implementation of IETF DiffServ-aware MPLS Traffic Engineering. However, it is in line with the requirements described in the first document above.The concept of "Class-Type" defined in that IETF draft corresponds to the concept of bandwidth pool implemented by DS-TE. And because DS-TE supports two bandwidth pools (global pool and sub-pool), DS-TE should be seen as supporting two Class-Types (Class-Type 0 and Class-Type 1).

Prerequisites

Your network must support the following Cisco IOS features in order to support guaranteed bandwidth services based on Diff-Serv-aware Traffic Engineering:

- MPLS
- IP Cisco Express Forwarding (CEF)
- OSPF or ISIS
- RSVP-TE
- QoS

Configuration Tasks

This section lists the minimum set of commands you need to implement the Diff-Serv-aware Traffic Engineering feature--in other words, to establish a tunnel that reserves bandwidth from the sub-pool.

The subsequent "Configuration Examples" section (page 14), presents these same commands in context and shows how, by combining them with QoS commands, you can build guaranteed bandwidth services.

New Commands

DS-TE commands were developed from the existing command set that configures MPLS traffic engineering. The only difference introduced to create DS-TE was the expansion of two commands:

- **ip rsvp bandwidth** was expanded to configure the size of the sub-pool on every link.
- **tunnel mpls traffic-eng bandwidth** was expanded to enable a TE tunnel to reserve bandwidth from the sub-pool.

The ip rsvp bandwidth command

The old command was

```
ip rsvp bandwidth x y
```

where x = the size of the only possible pool, and y = the size of a single traffic flow (ignored by traffic engineering)

Now the extended command is

```
ip rsvp bandwidth x y sub-pool z
```

where x = the size of the global pool, and z = the size of the sub-pool.

(Remember, the sub-pool's bandwidth is less than--because it is part of--the global pool's bandwidth.)

The tunnel mpls traffic-eng bandwidth command

The old command was

```
tunnel mpls traffic-eng bandwidth b
```

where b = the amount of bandwidth this tunnel requires.

Now you specify from which pool (global or sub) the tunnel's bandwidth is to come. You can enter

```
tunnel mpls traffic-eng bandwidth sub-pool b
```

This indicates that the tunnel should use bandwidth from the sub-pool. Alternatively, you can enter

```
tunnel mpls traffic-eng bandwidth b
```

This indicates that the tunnel should use bandwidth from the global pool (the default).

Note As can be seen in the Guaranteed Bandwidth Service Examples section (page 24), when QoS commands are added to DS-TE commands, guaranteed bandwidth tunnels can be created. To accomplish that across an MPLS ATM cloud, two more commands were created (beginning with Release 12.2(8)T): **mpls traffic-eng atm cos global-poo l** and **mpls traffic-eng atm cos sub-pool**.

The Configuration Procedure

To establish a sub-pool TE tunnel, you must enter configurations at three levels:

- the device (router, switch router, or label switch router)
- the physical interface (network interface)
- the tunnel interface

On the first two levels, you activate traffic engineering (and certain ATM settings if the tunnel will cross an ATM cloud). On the third level--the tunnel interface--you establish the sub-pool tunnel. Therefore, it is only at the tunnel headend device that you need to configure all three levels. At the tunnel midpoints and tail, it is sufficient to configure the first two levels.

In the tables below, each command is explained in brief. For a more complete explanation of any command, refer to the page given in the right-hand column.

Level 1: Configuring the Device

At this level, you tell the device (router or switch router) to use accelerated packet-forwarding (known as Cisco Express Forwarding or CEF), MultiProtocol Label Switching (MPLS), traffic-engineering tunneling, and either the OSPF or IS-IS routing algorithm (Open Shortest Path First or Intermediate System to Intermediate System). This level is often called global configuration mode because the configuration is applied globally, to the entire device, rather than to a specific interface or routing instance.

You enter the following commands:

SUMMARY STEPS

1. Router(config)# **ip cef**
2. Router(config)# **mpls traffic-eng tunnels**
3. Router(config)# **mpls traffic-eng atm cos sub-pool**
4. Router(config)# **router ospf**
5. Router (config-router)# **net** *network-entity-title*
6. Router (config-router)# **metric-style wide**
7. Router (config-router)# **is-type level** *-n*
8. Router (config-router)# **mpls traffic-eng level** *-n*
9. Router (config-router)# **passive-interface loopback0**
10. Router(config-router)# **mpls traffic-eng router-id loopback0**
11. Router(config-router)# **mpls traffic-eng area** *num*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **ip cef**	Enables CEF--which accelerates the flow of packets through the device.
Step 2	Router(config)# **mpls traffic-eng tunnels**	Enables MPLS, and specifically its traffic engineering tunnel capability.
Step 3	Router(config)# **mpls traffic-eng atm cos sub-pool** **Example:** **Example:** **Example:** `Router(config)#` **mpls traffic-eng atm cos global-pool**	[To be used only on ATM-LSR devices that are midpoints of a DS-TE tunnel]. Maps the queue carrying sub-pool traffic onto the highest cell-based class of service. (Optional). Maps the queue carrying global pool traffic onto one of the remaining three classes of service.
Step 4	Router(config)# **router ospf** **Example:** **Example:**	Invokes the OSPF routing process for IP and puts the device into router configuration mode. Proceed now to Steps 10and 11. Alternatively, you may invoke the ISIS routing process with this command and continue with Step 5.

	Command or Action	Purpose
	Example: [or] **Example:** Router(config)# **router isis**	
Step 5	Router (config-router)# **net** *network-entity-title*	Specifies the IS-IS network entity title (NET) for the routing process.
Step 6	Router (config-router)# **metric-style wide**	Enables the router to generate and accept IS-IS new-style TLVs (type, length, and value objects).
Step 7	Router (config-router)# **is-type level** *-n*	Configures the router to learn about destinations inside its own area or "IS-IS level".
Step 8	Router (config-router)# **mpls traffic-eng level** *-n*	Specifies the IS-IS level (which must be the same level as in the preceding step) to which the router will flood MPLS traffic-engineering link information.
Step 9	Router (config-router)# **passive-interface loopback0**	Instructs IS-IS to advertise the IP address of the loopback interface without actually running IS-IS on that interface. Continue with Step 10 but don't do Step 11--because Step 11 refers to OSPF.
Step 10	Router(config-router)# **mpls traffic-eng router-id loopback0**	Specifies that the traffic engineering router identifier is the IP address associated with the *loopback0* interface.
Step 11	Router(config-router)# **mpls traffic-eng area** *num*	Turns on MPLS traffic engineering for a particular OSPF area.

Level 2: Configuring the Network Interface

Having configured the device, you now must configure the interface on that device through which the tunnel will run. To do that, you first put the router into interface-configuration mode.

You then enable Resource Reservation Protocol (RSVP). RSVP is used to signal (set up) a traffic engineering tunnel, and to tell devices along the tunnel path to reserve a specific amount of bandwidth for the traffic that will flow through that tunnel. It is with this command that you establish the maximum size of the sub-pool.

Finally, you enable the MPLS traffic engineering tunnel feature on this network interface--and if you will be relying on the IS-IS routing protocol, you enable that as well. (In the case of ATM-PVC and LC-ATM interfaces you must enable IS-IS on a *sub* -interface level, and you must enable MPLS on *both* the interface and the sub-interface levels.)

To accomplish these tasks, you enter the following commands. (Step 7 or 8 is entered only when the interface you are configuring is either an ATM-PVC - Step 7 - or an LC-ATM - Step 8).

SUMMARY STEPS

1. Router(config)# **interface** *interface-id*
2. Router(config-if)# **ip rsvp bandwidth** *interface-kbps* **sub-pool** *kbps*
3. Router(config-if)# **mpls traffic-eng tunnels**
4. Router(config-if)# **interface** *interface-id.int-sub* **[mpls]**
5. Router(config-subif)# **ip rsvp bandwidth** *interface-kbps* **sub-pool** *kbps*
6. Router(config-subif)# **mpls traffic-eng tunnels**
7. Router(config-subif)# **atm pvc** *vcd vpi vci aal5snap*
8. Router(config-subif)# **mpls atm** *vpi-vpi*
9. Router(config-subif)# **ip router isis**
10. Router(config-subif)# **exit**
11. Router(config-if)# **ip router isis**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface** *interface-id*	Moves configuration to the interface level, directing subsequent configuration commands to the specific interface identified by the *interface-id*.
Step 2	Router(config-if)# **ip rsvp bandwidth** *interface-kbps* **sub-pool** *kbps*	Enables RSVP on this interface and limits the amount of bandwidth RSVP can reserve on this interface. The sum of bandwidth used by all tunnels on this interface cannot exceed *interface-kbps,* and the sum of bandwidth used by all sub-pool tunnels cannot exceed sub-pool *kbps*.
Step 3	Router(config-if)# **mpls traffic-eng tunnels**	Enables the MPLS traffic engineering tunnel feature on this interface. If the tunnel will go through an ATM-PVC or LC-ATM interface, continue on through Steps 4 through 11. However, if the tunnel will go through a POS interface, skip immediately to Step 11.
Step 4	Router(config-if)# **interface** *interface-id.int-sub* **[mpls]**	Moves configuration to the sub-interface level, directing subsequent configuration commands to the specific sub-interface identified by the *interface-id.sub-int*. Needed when the tunnel will traverse an ATM-PVC or LC-ATM interface. The keyword **mpls** is needed only with the LC-ATM interface.
Step 5	Router(config-subif)# **ip rsvp bandwidth** *interface-kbps* **sub-pool** *kbps*	Enables RSVP on the sub-interface and limits the amount of bandwidth RSVP can reserve on the sub-interface. The sum of bandwidth used by all tunnels on this sub-interface cannot exceed *interface-kbps,* and the sum of bandwidth used by all sub-pool tunnels cannot exceed sub-pool *kbps*.
Step 6	Router(config-subif)# **mpls traffic-eng tunnels**	Enables the MPLS traffic engineering tunnel feature on this sub-interface. If interface is ATM-PVC, continue with Step 7. If instead the interface is LC-ATM, skip to Step 8.]
Step 7	Router(config-subif)# **atm pvc** *vcd vpi vci aal5snap*	Sets the ATM PVC descriptor, path identifier, and channel identifier. Also sets the encapsulation as AAL5SNAP. [Now skip ahead to Step 9.]

	Command or Action	Purpose
Step 8	Router(config-subif)# **mpls atm** *vpi-vpi*	Sets the range of Virtual Path Identifiers on the LC-ATM interface.
Step 9	Router(config-subif)# **ip router isis**	Enables the IS-IS routing protocol on the sub-interface. Do not enter this command if you are configuring for OSPF.
Step 10	Router(config-subif)# **exit**	Exits the sub-interface level, returning to the interface level.
Step 11	Router(config-if)# **ip router isis**	If you are configuring an interface that does not have sub-interfaces, like POS, you enable IS-IS routing protocol at this step, on the interface level. (More on page 68.) Do not enter this command if you are configuring for OSPF.

Level 3: Configuring the Tunnel Interface

Now you create a set of attributes for the tunnel itself; those attributes are configured on the "tunnel interface" (not to be confused with the network interface just configured above).

The only command at this level which was affected to create DS-TE is **tunnel mpls traffic-eng bandwidth** (described in detail on page 145).

You enter the following commands:

SUMMARY STEPS

1. Router(config)# **interface tunnel1**
2. Router(config-if)# **tunnel destination** *A.B.C.D*
3. Router(config-if)# **tunnel mode mpls traffic-eng**
4. Router(config-if)# **tunnel mpls traffic-eng bandwidth**{**sub-pool** | [**global**]} *bandwid*th
5. Router(config-if)# **tunnel mpls traffic-eng priority**
6. Router(config-if)# **tunnel mpls traffic-eng path-option**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface tunnel1**	Creates a tunnel interface (named in this example **tunnel1**) and enters interface configuration mode. (More on page 62.)
Step 2	Router(config-if)# **tunnel destination** *A.B.C.D* **Example:**	Specifies the IP address of the tunnel tail device. (More on page 139.)
Step 3	Router(config-if)# **tunnel mode mpls traffic-eng**	Sets the tunnel's encapsulation mode to MPLS traffic engineering. (More on page 141.)

	Command or Action	Purpose
Step 4	Router(config-if)# **tunnel mpls traffic-eng bandwidth**{**sub-pool** | [**global**]} *bandwid*th	Configures the tunnel's bandwidth and assigns it either to the sub-pool or the global pool. (More on page 145).
Step 5	Router(config-if)# **tunnel mpls traffic-eng priority**	Sets the priority to be used when system determines which existing tunnels are eligible to be preempted. (More on page 148).
Step 6	Router(config-if)# **tunnel mpls traffic-eng path-option**	Configures the paths (hops) a tunnel should use. The user can enter an explicit path (can specify the IP addresses of the hops) or can specify a dynamic path (the router figures out the best set of hops). (More on page 147).

ATM-LSR Special Case

Because of the joint nature of the ATM-LSR device--being both a router running Cisco IOS and an ATM switch running its own, different operating system--distinct configuration tasks are required to have this device convey DS-TE tunnels across itself as a tunnel midpoint. (The ATM-LSR device cannot be the head nor tail of a DS-TE tunnel, only a midpoint).

Configuring the ATM-LSR midpoint device thus involves four tasks:

- Configuring a link between the router portion of the device and the switch portion
- Mapping router-level traffic pools to switch-level classes of service
- Mapping logical interfaces on the router to physical ports on the switch (the results are called XTagATM interfaces)
- Configuring resources within the switch (using the switch's own command language to address its operating system, different from Cisco IOS).

Establishing a link between the router and the switch control port

SUMMARY STEPS

1. Router(config)# **interface atm4/1 0/0/0**
2. Router(config-if)# **label-control-protocol vsi**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm4/1 0/0/0**	Moves configuration to the interface level, directing subsequent configuration commands to a Virtual Switch Interface on the router portion of the device. (More on page 62.)

	Command or Action	Purpose
Step 2	Router(config-if)# **label-control-protocol vsi** **Example:**	Enables Virtual Switch Interface protocol as the means of communication between the router interface and the switch's control port.

What to Do Next

Mapping pools to classes of service

SUMMARY STEPS

1. Router(config)# **mpls traffic-eng atm cos sub-pool**
2. Router(config)# **mpls traffic-eng atm cos global-pool**[available | standard | premium]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **mpls traffic-eng atm cos sub-pool**	Directs all sub-pool traffic entering the ATM-LSR to exit as the highest priority ATM class of service. (More on page 78.)
Step 2	Router(config)# **mpls traffic-eng atm cos global-pool**[available | standard | premium]	(Optional). Directs all global pool traffic entering the ATM-LSR to exit as one of the remaining three classes of service. (More on page 77.) If you don't use this command, the default, lowest priority service--"**available**"--is assigned.

What to Do Next

Mapping switch ports and configuring XTag-ATM interfaces

SUMMARY STEPS

1. Router(config)# **interface Xtagatm22**
2. Router(config-if)# **extended-port atm4/1 0/0/0 bpx2.2**
3. Router(config-if)# **ip address 10.1.1.2 255.0.0.0**
4. Router(config-if)# **ip rsvp bandwidth***interface-kbps***sub-pool** *kbps*
5. Router(config-if)# **mpls traffic-eng tunnels**
6. Router(config-if)# **mpls atm** *vpi-vpi*
7. Router(config-if)# **ip router isis**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface Xtagatm22** **Example:**	Moves configuration to the interface level, directing subsequent configuration commands to the specified XTag-ATM interface. (More on page 62.)
Step 2	Router(config-if)# **extended-port atm4/1 0/0/0 bpx2.2**	Associates a port on the switch with this XTagATM interface. extended-port ctrl-if { bpxport.number | igxport.number | descriptor vsi-descriptor | vsi vsi-port-number}
Step 3	Router(config-if)# **ip address 10.1.1.2 255.0.0.0**	Gives a network IP address to the XTagATM interface.
Step 4	Router(config-if)# **ip rsvp bandwidth***interface-kbps***sub-pool** *kbps* **Example:**	Enables RSVP on the XTagAtm interface and limits the amount of bandwidth RSVP can reserve on the interface. The sum of bandwidth used by all tunnels on this interface cannot exceed *interface-kbps,* and the sum of bandwidth used by all sub-pool tunnels cannot exceed sub-pool *kbps*. (More on page 69.)
Step 5	Router(config-if)# **mpls traffic-eng tunnels**	Enables the MPLS traffic engineering tunnel feature on this interface. (More on page 88.)
Step 6	Router(config-if)# **mpls atm** *vpi-vpi*	Sets the range of Virtual Path Identifiers on this interface. (More on page 138.)
Step 7	Router(config-if)# **ip router isis**	Enables the IS-IS routing protocol on this interface. (More on page 68.) Do not enter this command if you are configuring for OSPF.

Configuring resources within the switch

(Reminder--the following commands are entered directly into the switch. They are not part of the router portion's Cisco IOS software.)

SUMMARY STEPS

1. BPX-12# **uptrk***slot.port[.vtrk]*
2. BPX-12# **addshelf***slot.port.* **v***slot.port.*
3. BPX-12# **cnfrsrc** *slot.port.vtrk maxpvclcns maxpvcbw y/n partition e/d minvsilcns maxvsilcns vsistartvpi vsiendvpi vsiminbw*

DETAILED STEPS

	Command or Action	Purpose
Step 1	BPX-12# **uptrk***slot.port[.vtrk]* **Example:**	Activates a trunk, to generate framing. (The optional virtual trunk specification--*vrtk* -- is not used in our example).
Step 2	BPX-12# **addshelf***slot.port.* **v***slot.port.* **Example:**	Creates an interface shelf, to drive ATM cells to and from the switch.
Step 3	BPX-12# **cnfrsrc** *slot.port.vtrk maxpvclcns maxpvcbw y/n partition e/d minvsilcns maxvsilcns vsistartvpi vsiendvpi vsiminbw* **Example:** *vsimaxbw*	Configures resources for ports and trunks.

Verifying the Configurations

To view the complete configuration you have entered, use the EXEC command **show running-config** and check its output display for correctness.

To check *just one tunnel*'s configuration , enter **show interfaces tunnel** followed by the tunnel interface number. And to see that tunnel's RSVP bandwidth and flow, enter **show ip rsvp interface** followed by the name or number of the network interface (and also, in the case of an ATM-PVC or LC-ATM interface, the name or number of the sub-interface).

Here is an example of the information displayed by these two commands. To see an explanation of each field used in the following displays turn to page 95 for **show interfaces tunnel** and page 109 for **show ip rsvp interface**.

```
RTR1#show interfaces tunnel 4
Tunnel4 is up, line protocol is down
  Hardware is Routing Tunnel
  MTU 1500 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set, keepalive set (10 sec)
  Tunnel source 0.0.0.0, destination 0.0.0.0
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets, 0 restarts
RTR1#show ip rsvp interface pos4/0
interface    allocated  i/f max  flow max sub max
PO4/0        300K       466500K  466500K  0M
RTR1#show ip rsvp interface atm3/0
RTR1#show ip rsvp interface atm3/0.5
interface    allocated  i/f max  flow max sub max
AT3/0.5  110M  130M  130M  100
```

To view *all tunnels at once* on the router you have configured, enter **show mpls traffic-eng tunnels brief**. The information displayed when tunnels are functioning properly looks like this (a table explaining the display fields begins on page 136):

```
RTR1#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process:           running
RSVP Process:                  running
Forwarding:                    enabled
Periodic reoptimization:       every 3600 seconds, next in 3029 seconds
TUNNEL NAME  DESTINATION      UP IF     DOWN IF   STATE/PROT
RTR1_t0  192.168.1.13     -         SR3/0     up/up
RTR1_t1  192.168.1.13     -         SR3/0     up/up
RTR1_t2  192.168.1.13     -         PO4/0     up/up
[[RTR1_t3  192.168.1.13     -         AT3/0.5  up/up]]
Displayed 4(of 4) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

When one or more tunnels are not functioning properly, the display could instead look like this. (In the following example, tunnels t0 and t1 are down, as indicated in the far right column).

```
RTR1#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 2279 seconds
TUNNEL NAME  DESTINATION      UP IF     DOWN IF   STATE/PROT
RTR1_t0  192.168.1.13     -         SR3/0     up/down
RTR1_t1  192.168.1.13     -         SR3/0     up/down
RTR1_t2  192.168.1.13     -         PO4/0     up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

To find out *why* a tunnel is down, insert its name into this same command, after adding the keyword **name** and omitting the keyword **brief**. For example:

```
RTR1#show mpls traffic-eng tunnels name RTR1_t0

Name:RTR1_t0                            (Tunnel0) Destination:192.168.1.13
```

```
   Status:
     Admin:up         Oper:down  Path: not valid       Signalling:connected
```

If, as in this example, the Path is displayed as **not valid**, use the **show mpls traffic-eng topology** commandto make sure the router has received the needed updates. (That command is described on page 133.)

Additionally, you can use any of the following **show** commands to inspect particular aspects of the network, router, or interface concernef:

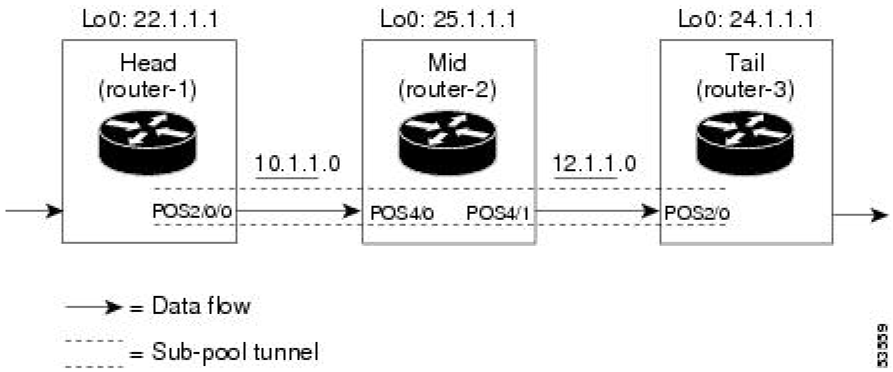
To see information about...	Use this command	
this level	and this item...	
Network	Advertised bandwidth allocation information	**show mpls traffic-eng link-management advertisements** (described on page 121)
	Preemptions along the tunnel path	**debug mpls traffic-eng link-management preemption** (described on page 61)
	Available TE link band- width on all head routers	**show mpls traffic-eng topology** (described on page 133)
Router	Status of all tunnels cur- rently signalled by this router	**show mpls traffic-eng link-management admission-control** (described on page 119)
	Tunnels configured on midpoint routers	**show mpls traffic-eng link-management summary** (described on page 131)
Interface	Detailed information on current bandwidth pools	**show mpls traffic-eng link-management bandwidth-allocation [interface-name**] (described on page 124
	TE RSVP bookkeeping	**show mpls traffic-eng link-management interfaces** (described on page 129)
	Entire configuration of one interface	**show run interface**

Configuration Examples

First this section presents the DS-TE configurations needed to create the sub-pool tunnel. Then it presents the more comprehensive design for building end-to-end guaranteed bandwidth service, which involves configuring Quality of Service as well.

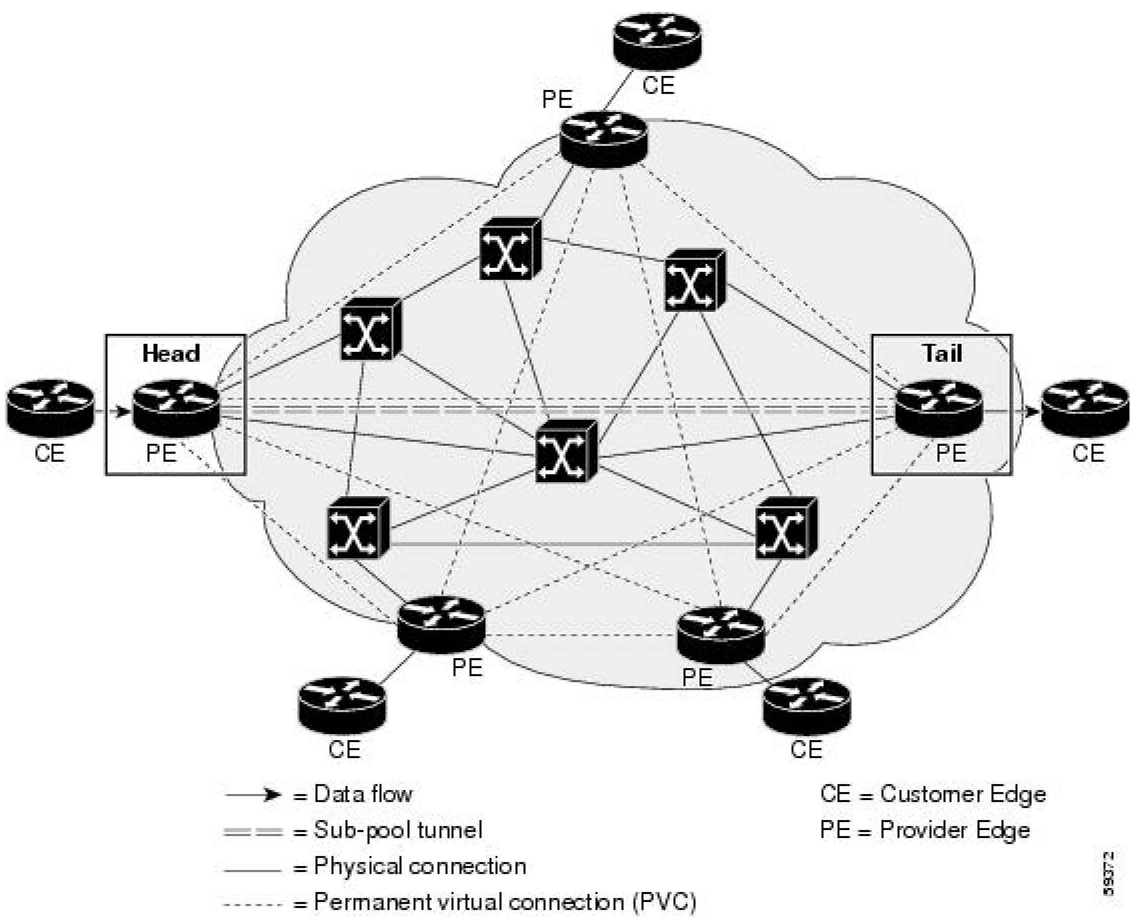
As shown in the figure below, the tunnel configuration involves at least three devices--tunnel head, midpoint, and tail. On each of those devices one or two network interfaces must be configured, for traffic ingress and egress.

Figure 25: Sample Tunnel Topology using POS Interfaces



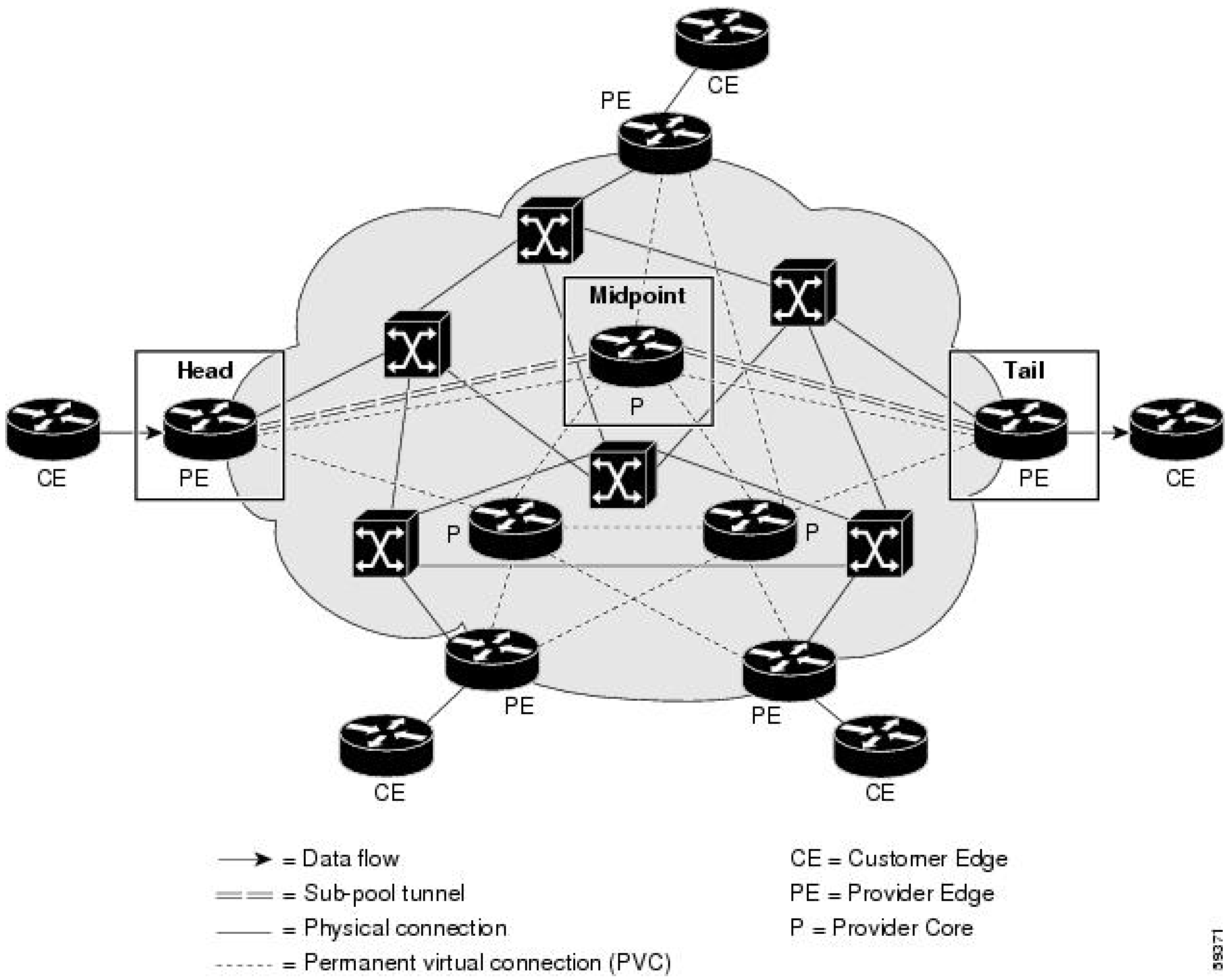
Sample topologies when the tunnel will run over ATM-PVCs are shown in the next two figures below.

Figure 26: Sample Tunnel across ATM-PVC Interfaces -- Full Mesh Topology



The full mesh topology shows no Midpoint device because the sub-pool tunnel can be routed along a direct PVC connecting the Head and Tail devices. However, if that particular PVC does not contain enough bandwidth, the tunnel can pass through alternate PVCs which may connect one or more PE routers. In that case the alternate PE router(s) will function as tunnel midpoint(s), and must be configured as shown in the Midpoint sections of the following configuration examples.

Figure 27: Sample Tunnel across ATM-PVC Interfaces -- Partial Mesh Topology

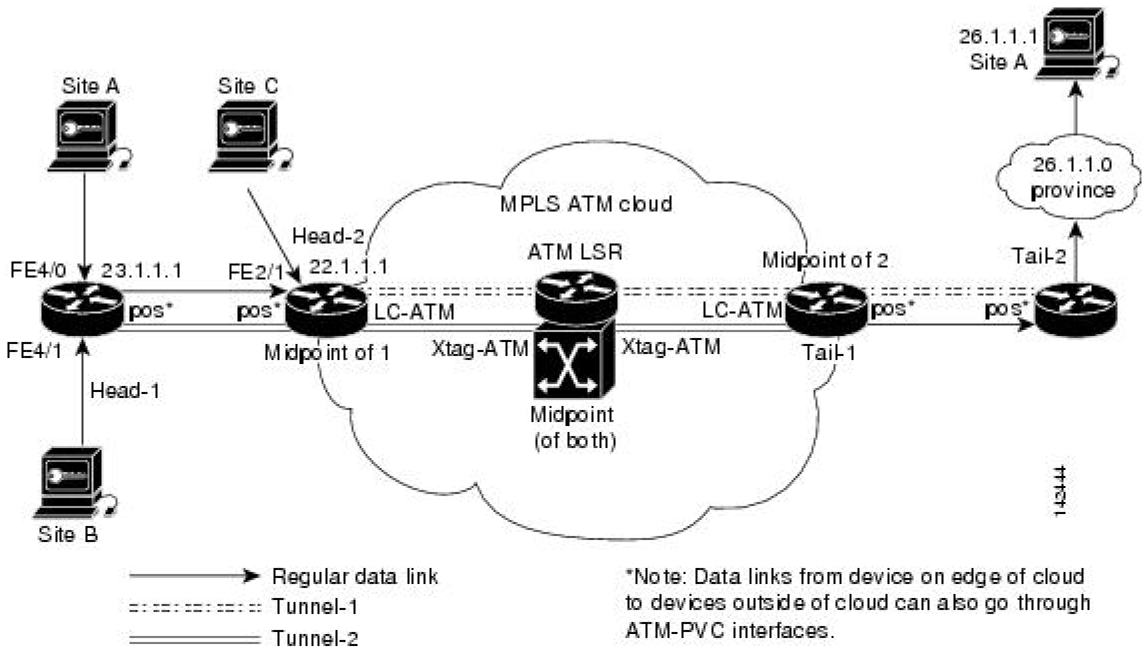


As shown in the figure below, DS-TE tunnels that travel through an MPLS ATM cloud can start either at a device outside the cloud or at one located on the edge of the cloud. Likewise, these tunnels can end either at a device on the edge of the cloud or one that is wholly outside the cloud. However, DS-TE tunnels cannot begin or end *inside* an MPLS ATM cloud.

On the edge of the cloud, the interface conveying the tunnel is an LC-ATM. Within the cloud, it is an XTag-ATM, residing on an ATM-LSR device.

A sample topology for tunnels that traverse LC-ATM interfaces is shown in the figure below

Figure 28: Sample Tunnels across LC-ATM Interfaces



The following example refers to all three figures. Where the language is specific to only one type of interface, that fact is indicated.

Tunnel Head

At the device level:

```
router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# ip cef
router(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router(config)# **router isis**	**router ospf 100**
router(config-router)# **net 49.0000.1000.0000.0010.00**	**redistribute connected**
router(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router(config-router)# **is-type level-1**	**network 22.1.1.1 0.0.0.0 area 0**
router(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**
router(config-router)# **passive-interface Loopback0**	

[now one resumes the common command set]:

```
router(config-router)# mpls traffic-eng router-id Loopback0
router(config-router)# exit
router(config)# interface Loopback0
```

At the virtual interface level:

```
router(config-if)# ip address 22.1.1.1 255.255.255.255
router(config-if)# no ip directed-broadcast
router(config-if)# exit
```

At the device level: [ATM cases appear on the left; POS case on the right]:

router(config)# **interface atm3/0**	**interface POS2/0/0**

[continuing each case at the network interface level (egress)]:

router(config-if)# **mpls traffic-eng tunnels**	**ip address 10.1.1.1 255.255.255.0**
router(config-if)# **ip rsvp bandwidth 130000 130000/ sub-pool 80000**	**mpls traffic-eng tunnels**
router(config-if)# **interface atm3/0.5** [append the keyword **mpls** if LC-ATM]	**ip rsvp bandwidth 130000 130000/ sub-pool 80000**
router(config-subif)# **ip address 10.1.1.1 255.255.255.0**	
router(config-subif)#**ip rsvp bandwidth 130000 130000 sub-pool 80000**	
router(config-subif)# **mpls traffic-eng tunnels**	
router(config-subif)# [if ATM-PVC]: **atm pvc 10 10 100 aal5snap** [if LC-ATM]: **mpls atm vpi 2-5**	
[if using IS-IS instead of OSPF]:	
router(config-subif)# **ip router isis**	
router(config-subif)# **exit**	
router(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router(config-if)# exit
```

At the device level:

```
router(config)# interface Tunnel1
```

At the tunnel interface level:

```
router(config-if)# bandwidth 110000
router(config-if)# ip unnumbered Loopback0
router(config-if)# tunnel destination 24.1.1.1
router(config-if)# tunnel mode mpls traffic-eng
router(config-if)# tunnel mpls traffic-eng priority 0 0
router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
```

```
router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
router(config-if)# exit
router(config)#
```

Midpoint Devices

At the device level:

```
router# configure terminal
router(config)# ip cef
router(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router(config)# **router isis**	**router ospf 100**
router(config-router)# **net 49.0000.1000.0000.0012.00**	**redistribute connected**
router(config-router)# **metric-style wide**	**network 11.1.1.0 0.0.0.255 area 0**
router(config-router)# **is-type level-1**	**network 12.1.1.0 0.0.0.255 area 0**
router(config-router)# **mpls traffic-eng level-1**	**network 25.1.1.1 0.0.0.0 area 0**
router(config-router)# **passive-interface Loopback0**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router(config-router)# mpls traffic-eng router-id Loopback0
router(config-router)# exit
router(config)# interface Loopback0
```

At the virtual interface level:

```
router(config-if)# ip address 25.1.1.1 255.255.255.255
router(config-if)# no ip directed-broadcast
router(config-if)# exit
```

[And if the device is an ATM-LSR:

```
router(config)#interface atm9/0 0/0/0
router(config-if)# label-control-protocol vsi
router(config-if)# exit
router(config)#mpls traffic-eng atm cos sub-pool
 ]
```

On all devices, for the ingress interface: [ATM-LSR appears on the left; ATM-PVC and LC-ATM cases in the middle; POS on the right]

router(config)# **interface Xtagatm22**	**interface atm3/0**	**interface POS4/0**

[continuing each case at the network interface level]

router(config-if)# **extended-port atm9/0 bpx2.2**	**mpls traffic-eng tunnels**	**ip address 11.1.1.2 255.255.255.0**
router(config-if)# **ip address 11.1.1.2 255.255.255.0**	**ip rsvp bandwidth 130000 130000/ sub-pool 80000**	**mpls traffic-eng tunnels**
router(config-if)# **ip rsvp bandwidth 130000 130000 sub-pool 80000**		**ip rsvp bandwidth 130000 130000/ sub-pool 80000**
router(config-if)# **mpls traffic-eng tunnels**		[If using IS-IS instead of OSPF]: **ip router isis**
router(config-if)# **mpls atm vpi 2-15**		
router(config-if)# **ip rsvp isis** [only if using IS-IS instead of OSPF]	**interface atm3/0.5** [append the keyword **mpls** if LC-ATM]	
router(config-subif)#	**ip address 11.1.1.2 255.255.255.0**	
router(config-subif)#	**ip rsvp bandwidth 130000 130000 sub-pool 80000**	
router(config-subif)#	**mpls traffic-eng tunnels**	
router(config-subif)#		

	[if ATM-PVC]: **atm pvc 10 10 100 aal5snap** [or if LC-ATM]: **mpls atm vpi 2-15**	
router(config-subif)#	[If using IS-IS instead of OSPF]: **ip router isis**	
router(config-subif)#	**exit**	

Continuing at the network interface level, regardless of interface type:

router(config-if)# **exit**

At the device level, for the egress interface: [ATM-LSR appears on the left; ATM-PVC and LC-ATM cases in the middle; POS on the right]

router(config)# **interface Xtagatm44**	**interface atm4/0**	**interface POS4/1**

[continuing each case at the network interface level]

router(config-if)# **extended-port atm9/0 bpx4.4**	**mpls traffic-eng tunnels**	**ip address 12.1.1.2 255.255.255.0**
router(config-if)# **ip address 12.1.1.2 255.255.255.0**	**ip rsvp bandwidth 130000 130000/ sub-pool 80000**	**mpls traffic-eng tunnels**
router(config-if)# **ip rsvp bandwidth 130000 130000 sub-pool 80000**		**ip rsvp bandwidth 130000 130000/ sub-pool 80000**
router(config-if)# **mpls traffic-eng tunnels**		[If using IS-IS instead of OSPF]: **ip router isis**
router(config-if)# **mpls atm vpi 2-15**		
router(config-if)# **ip router isis** [only if using IS-IS instead of OSPF]	**interface atm4/0.5** [append the keyword **mpls** if LC-ATM]	
router(config-subif)#	**ip address 12.1.1.2 255.255.255.0**	
router(config-subif)#	**ip rsvp bandwidth 130000 130000 sub-pool 80000**	
router(config-subif)#	**mpls traffic-eng tunnels**	
router(config-subif)#		

	[if ATM-PVC]: **atm pvc 10 10 100 aal5snap** [or if LC-ATM]: **mpls atm vpi 2-15**	
router(config-subif)#	[If using IS-IS instead of OSPF]: **ip router isis**	
router(config-subif)#	**exit**	

Continuing at the network interface level, regardless of interface type:

```
router(config-if)# exit
```

Note that there is no configuring of tunnel interfaces at the mid-point devices, only network interfaces, sub-interfaces, and the device globally.

When the midpoint device is an ATM-LSR, the following commands are also required. They are entered directly into the switch device, bypassing Cisco IOS:

```
BPX-12# uptrk 1.1
BPX-12# addshelf 1.1 v 1.1
BPX-12# cnfrsrc
 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
BPX-12# uptrk 2.2
BPX-12# cnfrsrc
 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000
BPX-12# uptrk 3.3
BPX-12# cnfrsrc
 3.3 256 252207 y 1 e 512 4096 2 5 26000 100000
BPX-12# uptrk 4.4
BPX-12# cnfrsrc
 4.4 256 252207 y 1 e 512 4096 2 5 26000 100000
BPX-12# uptrk 5.5
BPX-12# cnfrsrc
 5.5 256 252207 y 1 e 512 4096 2 5 26000 100000
```

Tail-End Device

At the device level:

```
router# configure terminal
router(config)# ip cef
router(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router(config)# **router isis**	**router ospf 100**
router(config-router)# **net 49.0000.1000.0000.0013.00**	**redistribute connected**
router(config-router)# **metric-style wide**	**network 12.1.1.0 0.0.0.255 area 0**
router(config-router)# **is-type level-1**	**network 24.1.1.1 0.0.0.0 area 0**
router(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**
router(config-router)# **passive-interface Loopback0**	

[now one resumes the common command set]:

```
router(config-router)# mpls traffic-eng router-id Loopback0
router(config-router)# exit
router(config)# interface Loopback0
```

At the virtual interface level:

```
router(config-if)# ip address 24.1.1.1 255.255.255.255
router(config-if)# no ip directed-broadcast
[and if using IS-IS instead of OSPF]:
router(config-if)# ip router isis
[and in all cases]:
router(config-if)# exit
```

At the device level: [ATM cases appear on the left; POS case on the right]:

router(config)# **interface atm2/0**	**interface POS2/0/0**

[continuing each case at the network interface level (ingress)]:

router(config-if)# **mpls traffic-eng tunnels**	**ip address 12.1.1.3 255.255.255.0**
router(config-if)# **ip rsvp bandwidth 130000 130000/ sub-pool 80000**	**mpls traffic-eng tunnels**
router(config-if)# **interface atm2/0.4** [append the keyword **mpls** if LC-ATM]	**ip rsvp bandwidth 130000 130000/ sub-pool 80000**
router(config-subif)# **ip address 12.1.1.3 255.255.255.0**	
router(config-subif)#**ip rsvp bandwidth 130000 130000 sub-pool 80000**	
router(config-subif)# **mpls traffic-eng tunnels**	
router(config-subif)# [if ATM-PVC]: **atm pvc 10 10 100 aal5snap** [if LC-ATM]: **mpls atm vpi 2-5**	
[if using IS-IS instead of OSPF]:	
router(config-subif)# **ip router isis**	
router(config-subif)# **exit**	
router(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router(config-if)# exit
```

Guaranteed Bandwidth Service Configuration

Having configured two bandwidth pools, you now can

- Use one pool, the sub-pool, for tunnels that carry traffic requiring strict bandwidth guarantees or delay guarantees
- Use the other pool, the global pool, for tunnels that carry traffic requiring only Differentiated Service.

Having a separate pool for traffic requiring strict guarantees allows you to limit the amount of such traffic admitted on any given link. Often, it is possible to achieve strict QoS guarantees only if the amount of guaranteed traffic is limited to a portion of the total link bandwidth.

Having a separate pool for other traffic (best-effort or diffserv traffic) allows you to have a separate limit for the amount of such traffic admitted on any given link. This is useful because it allows you to fill up links with best-effort/diffserv traffic, thereby achieving a greater utilization of those links.

Providing Strict QoS Guarantees Using DS-TE Sub-pool Tunnels

A tunnel using sub-pool bandwidth can satisfy the stricter requirements if you do all of the following:

1. Select a queue--or in diffserv terminology, select a PHB (per-hop behavior)--to be used exclusively by the strict guarantee traffic. This shall be called the "GB queue."

If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. On the Cisco 7200 it is the "priority" queue. You must configure the bandwidth of the queue to be at least equal to the bandwidth of the sub-pool.

If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used. On the Cisco 7200 you use one of the existing Class-Based Weighted Fair Queuing (CBWFQ) queues.

1. Ensure that the guaranteed traffic sent through the sub-pool tunnel is placed in the GB queue *at the outbound interface of every tunnel hop* , and that no other traffic is placed in this queue.

You do this by marking the traffic that enters the tunnel with a unique value in the mpls exp bits field, and steering only traffic with that marking into the GB queue.

1. Ensure that this GB queue is never oversubscribed; that is, see that no more traffic is sent into the sub-pool tunnel than the GB queue can handle.

You do this by rate-limiting the guaranteed traffic before it enters the sub-pool tunnel. The aggregate rate of all traffic entering the sub-pool tunnel should be less than or equal to the bandwidth capacity of the sub-pool tunnel. Excess traffic can be dropped (in the case of delay/jitter guarantees) or can be marked differently for preferential discard (in the case of bandwidth guarantees).

1. Ensure that the amount of traffic entering the GB queue is limited to an appropriate percentage of the total bandwidth of the corresponding outbound link. The exact percentage to use depends on several factors that can contribute to accumulated delay in your network: your QoS performance objective, the total number of tunnel hops, the amount of link fan-in along the tunnel path, burstiness of the input traffic, and so on.

You do this by setting the sub-pool bandwidth of each outbound link to the appropriate percentage of the total link bandwidth (that is, by adjusting the z parameter of the **ip rsvp bandwidth** command).

Providing Differentiated Service Using DS-TE Global Pool Tunnels

You can configure a tunnel using global pool bandwidth to carry best-effort as well as several other classes of traffic. Traffic from each class can receive differentiated service if you do all of the following:

1. Select a separate queue (a distinct diffserv PHB) for each traffic class. For example, if there are three classes (gold, silver, and bronze) there must be three queues (diffserv AF2, AF3, and AF4). [If the tunnel is to cross an MPLS ATM cloud, only one class of global pool traffic may be configured.]

2 Mark each class of traffic using a unique value in the MPLS experimental bits field (for example gold = 4, silver = 5, bronze = 6). [On the ATM-LSR, you specify the class of service desired **--premium**, **standard**, or the default service, **available**--using the command **mpls traffic-eng atm cos global-pool**].

3 Ensure that packets marked as Gold are placed in the gold queue, Silver in the silver queue, and so on. The tunnel bandwidth is set based on the expected aggregate traffic across all classes of service.

To control the amount of diffserv tunnel traffic you intend to support on a given link, adjust the size of the global pool on that link.

Providing Strict Guarantees and Differentiated Service in the Same Network

Because DS-TE allows simultaneous constraint-based routing of sub-pool and global pool tunnels, strict guarantees and diffserv can be supported simultaneously in a given network.

Guaranteed Bandwidth Service Examples

Given the many topologies in which Guaranteed Bandwidth Services can be applied, there is space here only to present two examples. They illustrate opposite ends of the spectrum of possibilities.

In the first example, the guaranteed bandwidth tunnel can be easily specified by its destination. So the forwarding criteria refer to a single destination prefix.

In the second example, there can be many final destinations for the guaranteed bandwidth traffic, including a dynamically changing number of destination prefixes. So the forwarding criteria are specified by Border Gateway Protocol (BGP) policies.

Example with Single Destination Prefix

The three figures below illustrate topologies for guaranteed bandwidth services whose destination is specified by a single prefix. In the first figure below, the interfaces to be configured are POS (Packet over SONET), while in second figure below the interfaces are ATM-PVC (Asynchronous Transfer Mode - Permanent Virtual Circuit), and in the third figure below, they are LC-ATM (Label Controlled - Asynchronous Transfer Mode) and, within the MPLS ATM cloud, XTag-ATM. In all three illustrations, the destination for the guaranteed bandwidth service is either a single host (like a voice gateway, here designated "Site D" and bearing prefix 26.1.1.1) or a subnet (like a web farm, here called "Province" and bearing prefix 26.1.1.0). Three services are offered in each sample topology:

- From Site A (defined as all traffic arriving at interface FE4/0): to host 26.1.1.1, 8 Mbps of guaranteed bandwidth with low loss, low delay and low jitter
- From Site B (defined as all traffic arriving at interface FE4/1): towards subnet 26.1.1.0, 32 Mbps of guaranteed bandwidth with low loss

- From Site C (defined as all traffic arriving at interface FE2/1): towards subnet 26.1.1.0, 30 Mbps of guaranteed bandwidth with low loss.

Figure 29: Sample Topology for Guaranteed Bandwidth Services (traversing POS interfaces) to a Single Destination Prefix

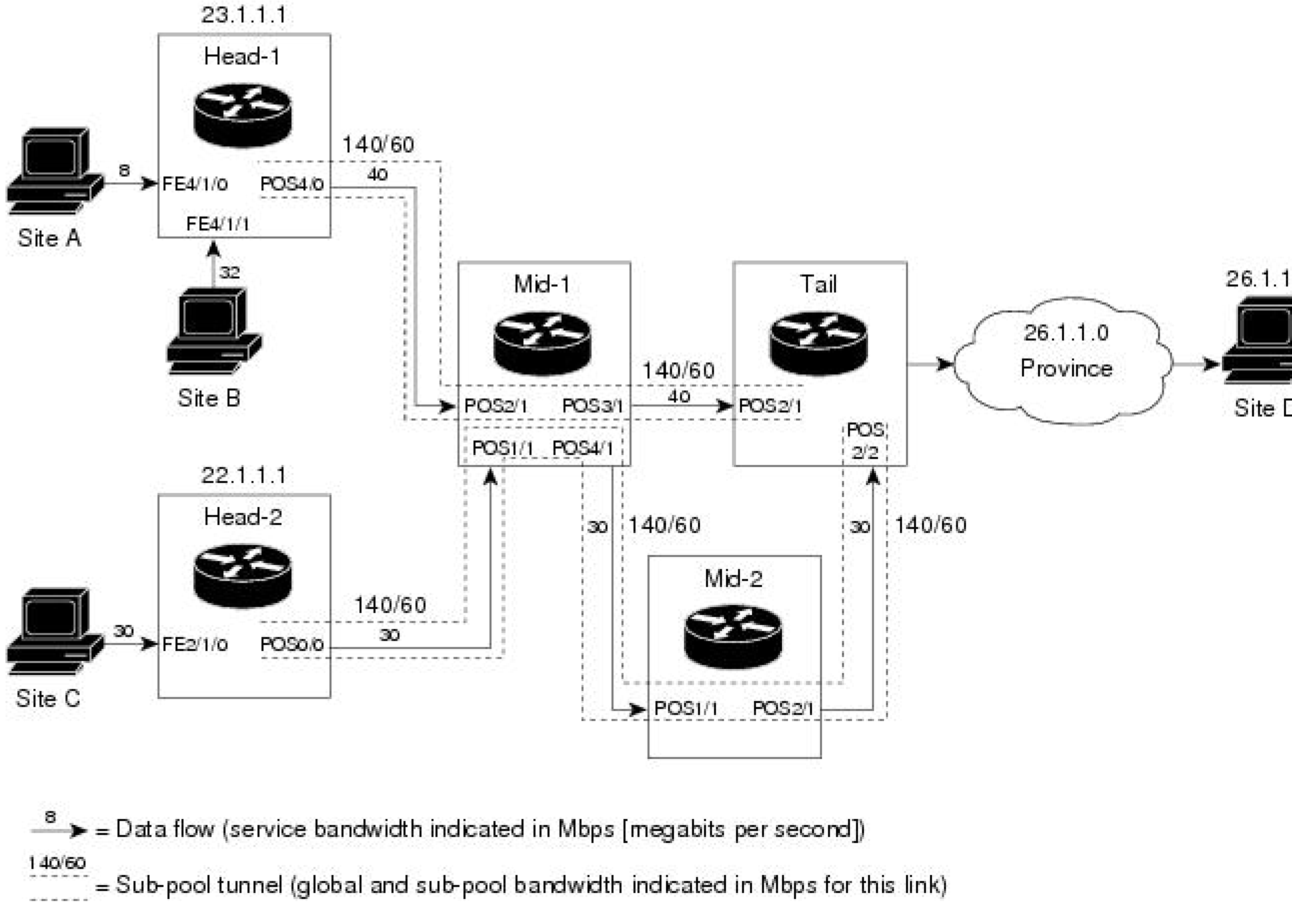


Figure 30: Sample Topology for Guaranteed Bandwidth Services (traversing ATM-PVC interfaces) to a Single Destination Prefix

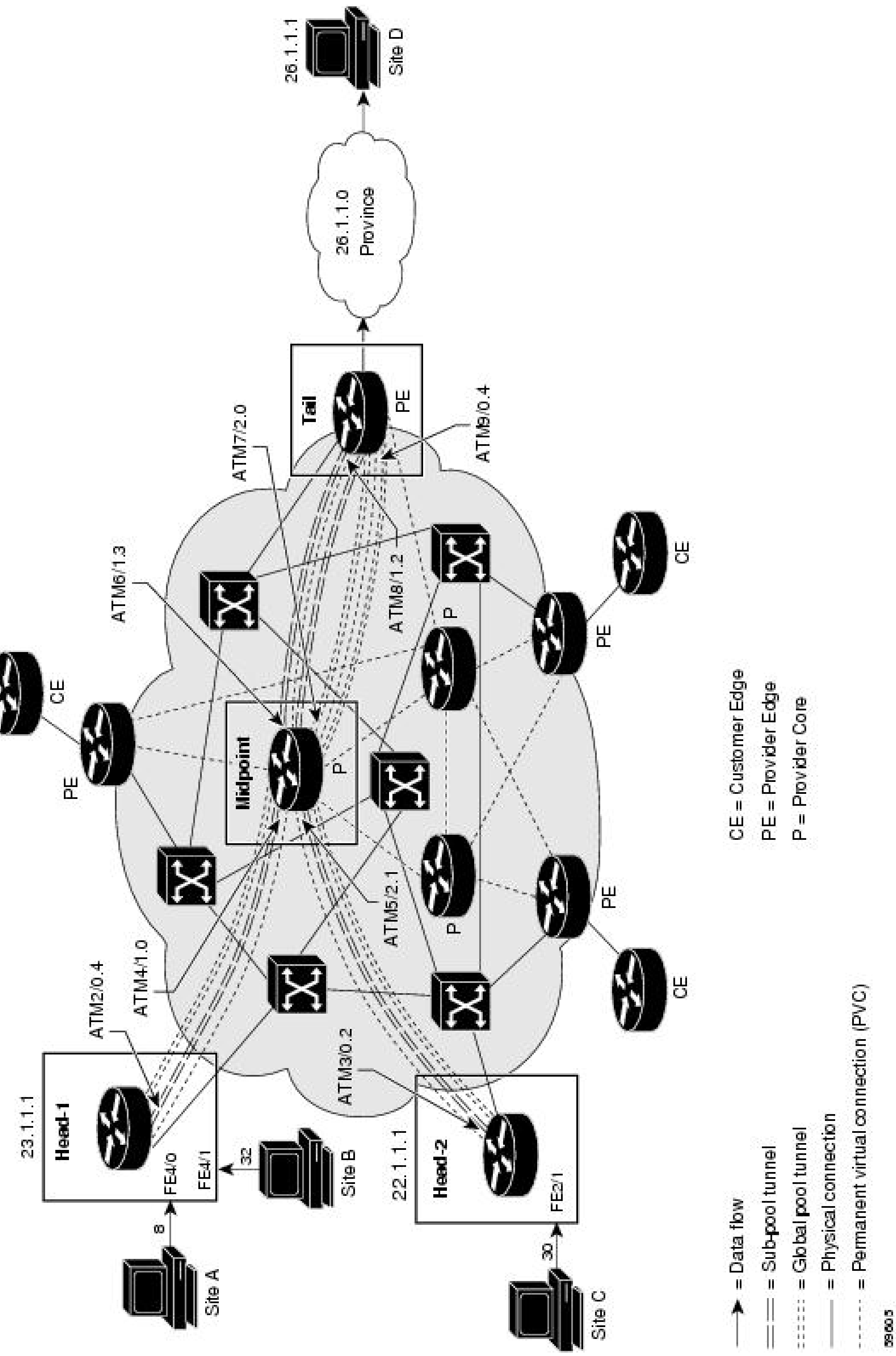
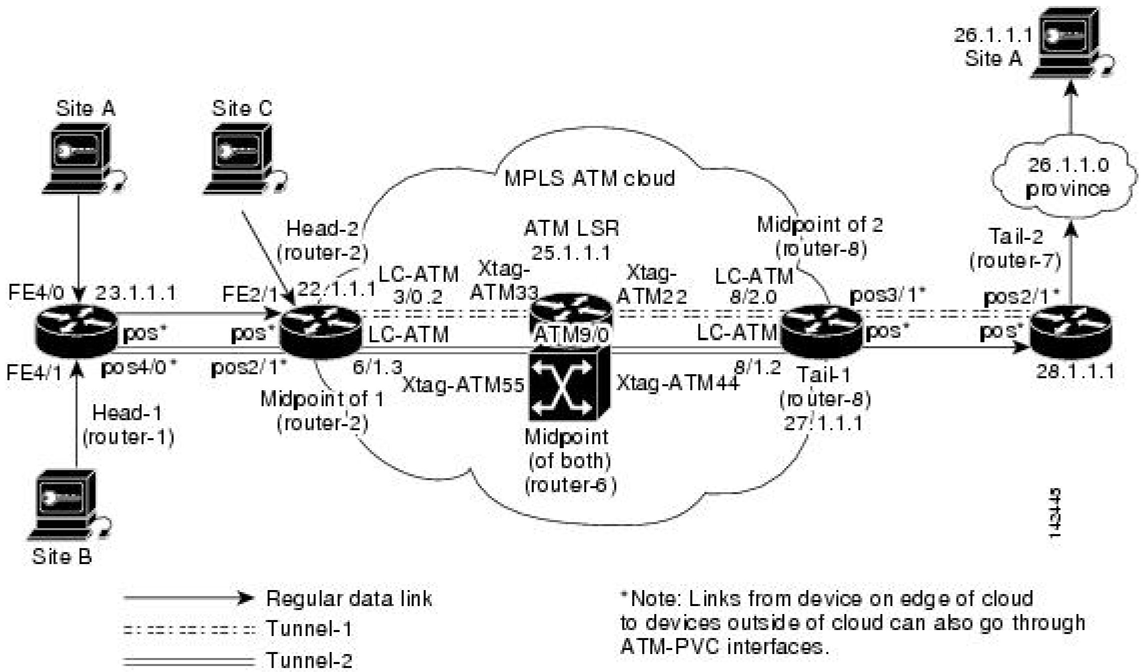

26.1.1.1
Site D
26.1.1.0
Province
Tail
PE
ATM7/2.0
ATM9/0.4
ATM6/1.3
ATM8/1.2
P
CE
PE
Midpoint
P
ATM2/0.4
ATM4/1.0
ATM5/2.1
ATM3/0.2
23.1.1.1
Head-1
FE4/0
FE4/1
32
Site B
8
Site A
22.1.1.1
Head-2
FE2/1
30
Site C
CE = Customer Edge
PE = Provider Edge
P = Provider Core
= Data flow
= Sub-pool tunnel
= Global pool tunnel
= Physical connection
= Permanent virtual connection (PVC)
59605

Figure 31: Sample Topology for Guaranteed Bandwidth Services (traversing LC-ATM and XTag-ATM interfaces) to a Single Destination Prefix



These three services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the router-4 tail (in our LC-ATM example, to tail router-8)
- From the Head-2 router, 22.1.1.1, to the router-4 tail (in our LC-ATM example, to tail router-7)

In the POS and ATM-PVC examples, both tunnels use the same tail router, though they have different heads. This is to illustrate that many combinations are possible. (In Figure 5 one midpoint router is shared by both tunnels. In the real world there could of course be many more midpoints.)

All POS, ATM-PVC, LC-ATM, and XTagATM interfaces in this example are OC3, whose capacity is 155 Mbps.

Configuring Tunnel Head-1

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier on page 14). Then we present the QoS commands that guarantee end-to-end service on the subpool tunnel. With the 7200 router, Modular QoS CLI is used.

Configuring the Pools and Tunnel

At the device level:

```
router-1(config)# ip cef
router-1(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# **router isis**	**router ospf 100**
router-1(config-router)# **net 49.0000.1000.0000.0010.00**	**redistribute connected**
router-1(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-1(config-router)# **is-type level-1**	**network 23.1.1.1 0.0.0.0 area 0**
router-1(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**
router-1(config-router)# **passive-interface Loopback0**	

[now one resumes the common command set]:

```
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
```

Create a virtual interface:

```
router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-1(config)# **interface atm2/0**	**interface POS4/0**

[then continue each case at the network interface level:

router-1(config-if)# **mpls traffic-eng tunnels**	**ip address 10.1.1.1 255.255.255.0**
router-1(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-1(config-if)# **interface atm2/0.4**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-1(config-subif)# **ip address 10.1.1.1 255.255.255.0**	
router-1(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-1(config-subif)# **mpls traffic-eng tunnels**	
router-1(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-1(config-subif)# **ip router isis**	
router-1(config-subif)# **exit**	
router-1(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-1(config-if)# exit
```

At the tunnel interface:

```
router-1(config)# interface Tunnel1
router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
```

To ensure that packets destined to host 26.1.1.1 and subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```
router-1(config)# ip route 26.1.1.0 255.255.255.0 Tunnel1
router-1(config)# exit
```

And in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```
router-1(config)# no tunnel mpls traffic-eng autoroute announce
```

For Service from Site A to Site D

At the inbound network interface (FE4/0):

SUMMARY STEPS

1. In global configuration mode, create a class of traffic matching ACL 100, called "sla-1-class":
2. Create an ACL 100 to refer to all packets destined to 26.1.1.1:
3. Create a policy named "sla-1-input-policy", and according to that policy:
4. The policy is applied to packets entering interface FE4/0.

DETAILED STEPS

Step 1 In global configuration mode, create a class of traffic matching ACL 100, called "sla-1-class":

Example:

```
class-map match-all sla-1-class
match access-group 100
```

Step 2 Create an ACL 100 to refer to all packets destined to 26.1.1.1:

Example:

```
access-list 100 permit ip any host 26.1.1.1
```

Step 3 Create a policy named "sla-1-input-policy", and according to that policy:
Packets in the class called "sla-1-class" are rate-limited to

- a rate of 8 million bits per second
- a normal burst of 1 million bytes
- a maximum burst of 2 million bytes

Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

Packets which exceed this rate are dropped.

All other packets are marked with experimental bit 0 and are forwarded.

Example:

```
policy-map sla-1-input-policy
class sla-1-class
police 8000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \ exceed-action drop
class class-default
set-mpls-exp-transmit 0
```

Step 4 The policy is applied to packets entering interface FE4/0.

Example:

```
interface FastEthernet4/0
service-policy input sla-1-input-policy
```

For Service from Site B to Subnet Province

At the inbound network interface (FE4/1):

SUMMARY STEPS

1. In global configuration mode, create a class of traffic matching ACL 120, called "sla-2-class":
2. Create an ACL, 120, to refer to all packets destined to subnet 26.1.1.0:
3. Create a policy named "sla-2-input-policy", and according to that policy
4. The policy is applied to packets entering interface FE4/1.

DETAILED STEPS

Step 1 In global configuration mode, create a class of traffic matching ACL 120, called "sla-2-class":

Example:

```
class-map match-all sla-2-class
match access-group 120
```

Step 2 Create an ACL, 120, to refer to all packets destined to subnet 26.1.1.0:

Example:

```
access-list 120 permit ip any 26.1.1.0 0.0.0.255
```

Step 3 Create a policy named "sla-2-input-policy", and according to that policy
Packets in the class called "sla-2-class" are rate-limited to:

- a rate of 32 million bits per second
- a normal burst of 1 million bytes
- a maximum burst of 2 million bytes

Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

Packets which exceed this rate are dropped.

All other packets are marked with experimental bit 0 and are forwarded.

Example:

```
policy-map sla-2-input-policy
class sla-2-class
police 32000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \ exceed-action drop
class class-default
set-mpls-exp-transmit 0
```

Step 4 The policy is applied to packets entering interface FE4/1.

Example:

```
interface FastEthernet4/1
service-policy input sla-2-input-policy
```

For Both Services

The outbound interface (POS4/0 in Figure 5 and Figure 7, and ATM2/0.4 in Figure 6) is configured as follows:

SUMMARY STEPS

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".
2. Create a policy named "output-interface-policy". According to that policy, packets in the class "exp-5-traffic" are put in the priority queue (which is rate-limited to 62 kbits/sec).
3. The policy is applied to packets exiting subinterface ATM2/0.4 (first example) or interface POS4/0 (second example):

DETAILED STEPS

Step 1 In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

Example:

```
class-map match-all exp-5-traffic
match mpls experimental 5
```

Step 2 Create a policy named "output-interface-policy". According to that policy, packets in the class "exp-5-traffic" are put in the priority queue (which is rate-limited to 62 kbits/sec).

Example:

```
policy-map output-interface-policy
```

```
class exp-5-traffic
priority 62
```

Step 3 The policy is applied to packets exiting subinterface ATM2/0.4 (first example) or interface POS4/0 (second example):

Example:

```
interface atm2/0
interface atm2/0.4
service-policy output output-interface-policy
```

Example:

```
interface POS4/0
service-policy output\ output-interface-policy
```

The result of the above configuration lines is that packets entering the router via interface FE4/0 destined to host 26.1.1.1, or entering the router via interface FE4/1 destined to subnet 26.1.1.0, will have their MPLS experimental bit set to 5. We assume that no other packets entering the router (on any interface) are using this value. (If this cannot be assumed, an additional configuration must be added to mark all such packets to another experimental value.) Packets marked with experimental bit 5, when exiting the router via interface POS4/0 or subinterface ATM2/0.4, will be placed into the priority queue.

Configuring Tunnel Head-2

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier on page 16). Then we present the QoS commands that guarantee end-to-end service on the subpool tunnel. With the 7200 router, Modular QoS CLI is used. [And because this router is on the edge of the MPLS ATM cloud in Figure 7, an LC-ATM interface is configured in that example.]

Configuring the Pools and Tunnel

At the device level:

```
router-2(config)# ip cef
router-2(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# **router isis**	**router ospf 100**
router-2(config-router)# **net 49.0000.1000.0000.0011.00**	**redistribute connected**
router-2(config-router)# **metric-style wide**	**network 11.1.1.0 0.0.0.255 area 0**
router-2(config-router)# **is-type level-1**	**network 22.1.1.1 0.0.0.0 area 0**
router-2(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**
router-2(config-router)# **passive-interface Loopback0**	

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# no ip directed-broadcast
router-2(config-if)# exit
```

For the outgoing network interface:

[ATM cases appear on the left; POS case on the right]:

router-2(config)# **interface atm3/0**	**interface POS0/0**

[then continue each case at the network interface level]:

router-2(config-if)# **mpls traffic-eng tunnels**	**ip address 11.1.1.1 255.0.0.0**
router-2(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-2(config-if)# **interface atm3/0.2** [append the keyword **mpls** if LC-ATM]	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-2(config-subif)# **ip address 11.1.1.1 255.0.0.0**	
router-2(config-subif)#**ip rsvp bandwidth 140000 140000 sub-pool 60000**	
router-2(config-subif)# **mpls traffic-eng tunnels**	
router-2(config-subif)# [if ATM-PVC]: **atm pvc 10 10 100 aal5snap** [if LC-ATM]: **mpls atm vpi 2-5**	
[if using IS-IS instead of OSPF]:	
router-2(config-subif)# **ip router isis**	
router-2(config-subif)# **exit**	
router-2(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-2(config-if)# exit
```

At the tunnel interface:

```
router-2(config)# interface Tunnel2
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1

[though in Figure 7:
tunnel destination 28.1.1.1
]
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
```

```
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
```

To ensure that packets destined to subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```
router-2(config)# ip route 26.1.1.0 255.255.255.0 Tunnel2
router-2(config)# exit
```

And in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```
router-2(config)# no tunnel mpls traffic-eng autoroute announce
```

For Service from Site C to Subnet Province

At the inbound network interface (FE2/1):

SUMMARY STEPS

1. In global configuration mode, create a class of traffic matching ACL 130, called "sla-3-class":
2. Create an ACL, 130, to refer to all packets destined to subnet 26.1.1.0:
3. Create a policy named "sla-3-input-policy", and according to that policy:
4. The policy is applied to packets entering interface FE2/1.
5. The outbound interface (POS0/0 or ATM3/0.2) is configured as follows:
6. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".
7. Create a policy named "output-interface-policy". According to that policy, packets in the class "exp-5-traffic" are put in the priority queue (which is rate-limited to 32 kbits/sec).
8. The policy is applied to packets exiting interface ATM3/0.2 (first example) or POS0/0 (second example):

DETAILED STEPS

Step 1 In global configuration mode, create a class of traffic matching ACL 130, called "sla-3-class":

Example:

```
class-map match-all sla-3-class
match access-group 130
```

Step 2 Create an ACL, 130, to refer to all packets destined to subnet 26.1.1.0:

Example:

```
access-list 130 permit ip any 26.1.1.0 0.0.0.255
```

Step 3 Create a policy named "sla-3-input-policy", and according to that policy:
Packets in the class called "sla-3-class" are rate-limited to:

- a rate of 30 million bits per second
- a normal burst of 1 million bytes
- a maximum burst of 2 million bytes

Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

Packets which exceed this rate are dropped.

All other packets are marked with experimental bit 0 and are forwarded.

Example:

```
policy-map sla-3-input-policy
class sla-3-class
police 30000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \ exceed-action drop
class class-default
set-mpls-exp-transmit 0
```

Step 4 The policy is applied to packets entering interface FE2/1.

Example:

```
interface FastEthernet2/1
service-policy input sla-3-input-policy
```

Step 5 The outbound interface (POS0/0 or ATM3/0.2) is configured as follows:

Step 6 In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

Example:

```
class-map match-all exp-5-traffic
match mpls experimental 5
```

Step 7 Create a policy named "output-interface-policy". According to that policy, packets in the class "exp-5-traffic" are put in the priority queue (which is rate-limited to 32 kbits/sec).

Example:

```
policy-map output-interface-policy
class exp-5-traffic
priority 32
```

Step 8 The policy is applied to packets exiting interface ATM3/0.2 (first example) or POS0/0 (second example):

Example:

```
interface atm3/0
interface atm3/0.2
service-policy output output-interface-policy
```

Example:

```
interface POS0/0
service-policy output\ output-interface-policy
```

The result of the above configuration lines is that packets entering the router via interface FE2/1 destined to subnet 26.1.1.0, will have their MPLS experimental bit set to 5. We assume that no other packets entering the router (on any interface) are using this value. (If this cannot be assumed, an additional configuration must be added to mark all such packets to another experimental value.) Packets marked with experimental bit 5, when exiting the router via interface POS0/0 or ATM3/0.2, will be placed into the priority queue.

Tunnel Midpoint Configurations

All four interfaces on the 7200 midpoint router ("**Mid-1**" in Figure 5, "**Midpoint**" in Figure 6) are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces).

When an ATM-LSR serves as a midpoint (as in Figure 7), its XTagATM interfaces and BPX or IGX switching resources must be configured. Also, two new MPLS commands are used. The details of this configuration are presented in the ATM-LSR section which begins on page 38.

The LC-ATM midpoint configuration (on the left edge of the ATM cloud in Figure 7) is presented on page 35. LC-ATM at a midpoint on the right edge of the cloud in Figure 7 is presented on page 39.

Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-3(config)# **router isis**	**router ospf 100**
router-3(config-router)# **net 49.0000.2400.0000.0011.00**	**redistribute connected**
router-3(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-3(config-router)# **is-type level-1**	**network 11.1.1.0 0.0.0.255 area 0**
router-3(config-router)# **mpls traffic-eng level-1**	**network 24.1.1.1 0.0.0.0 area 0**
router-3(config-router)# **passive-interface Loopback0**	**network 12.1.1.0 0.0.0.255 area 0**
router-3(config-router)#	**network 13.1.1.0 0.0.0.255 area 0**
router-3(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit
```

Create a virtual interface:

```
router-3(config)# interface Loopback0
router-3(config-if)# ip address 22.1.1.1 255.255.255.255
router-3(config-if)# exit
```

For one incoming network interface, first at the device level:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm4/1**	**interface POS2/1**

[then continue each case at the network interface level]:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 10.1.1.2 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm4/1.0**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-3(config-subif)# **ip address 10.1.1.2 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000 sub-pool 60000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	
router-3(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

For the other incoming network interface, first at the device level:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm5/2**	**interface POS1/1**

[then continuing each case at the network interface level]:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 11.1.1.2 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000/ sub-pool 60000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm5/2.1**	**ip rsvp bandwidth 140000 140000/ sub-pool 60000**
router-3(config-subif)# **ip address 11.1.1.2 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	
router-3(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

For one outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm6/1**	**interface POS3/1**

[then continue each case at the network interface level]:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 11.1.1.2 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm6/1.3**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-3(config-subif)# **ip address 11.1.1.2 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	
router-3(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

For the other outgoing network interface, first at the device level:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm7/2**	**interface POS3/1**

[then, continuing each case at the network interface level]:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 12.1.1.1 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm7/2.0**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-3(config-subif)# **ip address 12.1.1.1 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	
router-3(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

Tunnel Midpoint Configuration POS ingress and LC-ATM egress

Configuring the Pools and Tunnels

At the device level:

```
router-2(config)# ip cef
router-2(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# **router isis**	**router ospf 100**
router-2(config-router)# **net 49.0000.2400.0000.0011.00**	**redistribute connected**
router-2(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-2(config-router)# **is-type level-1**	**network 11.1.1.0 0.0.0.255 area 0**
router-2(config-router)# **mpls traffic-eng level-1**	**network 24.1.1.1 0.0.0.0 area 0**
router-2(config-router)# **passive-interface Loopback0**	**network 12.1.1.0 0.0.0.255 area 0**
router-2(config-router)#	**network 13.1.1.0 0.0.0.255 area 0**
router-2(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# exit
```

For the incoming network interface, first at the device level:

```
router-2(config)# interface POS2/1
```

[then continuing at the network interface level]:

```
router-2(config-if)# ip address 11.1.1.2 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
```

[If using IS-IS instead of OSPF]:

```
router-2(config-if)# ip router isis
[and in both cases]:
router-2(config-if)# exit
```

For the outgoing network interface:

```
router-2(config)# interface atm6/1
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-2(config-if)# interface atm6/1.3 mpls
router-2(config-subif)# ip address 11.1.1.2 255.0.0.0
```

```
router-2(config-subif)#ip rsvp bandwidth 140000 140000 sub-pool 60000
router-2(config-subif)# mpls traffic-eng tunnels
router-2(config-subif)# mpls atm vpi 2-15
[if using IS-IS instead of OSPF]:
router-2(config-subif)# ip router isis
router-2(config-subif)# exit
[and in bothcases]:
router-2(config-if)# exit
```

Tunnel Midpoint Configuration all POS

[For the sake of simplicity, the ATM-PVC example (Figure 6) was illustrated with only one midpoint router.]

Both interfaces on the second 7200 midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

Configuring the Pools and Tunnel

At the device level:

```
router-5(config)# ip cef
router-5(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-5(config)# **router isis**	**router ospf 100**
router-5(config-router)# **net 49.2500.1000.0000.0012.00**	**redistribute connected**
router-5(config-router)# **metric-style wide**	**network 13.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **is-type level-1**	**network 14.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **mpls traffic-eng level-1**	**network 25.1.1.1 0.0.0.0 area 0**
router-5(config-router)# **passive-interface Loopback0**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit
```

Create a virtual interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit
```

At the incoming network interface level:

```
router-5(config)# interface pos1/1
```

```
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

At the outgoing network interface level:

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

Tunnel Midpoint Configurationz all XTag-ATM

When an ATM-LSR serves as a midpoint, its Virtual Switch Interface, XTagATM interfaces, and BPX or IGX switching resources must be configured. Also, one or two new MPLS commands are used on the ATM-LSR (namely, **mpls traffic-eng atm cos sub-pool** and **mpls traffic-eng atm cos global-pool**), to transfer traffic from priority queues into class-of-service (since the cell-based switch cannot examine packets).

Configuring the Pools and Tunnel

At the device level:

```
router-6(config)# ip cef
router-6(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-6(config)# **router isis**	**router ospf 100**
router-6(config-router)# **net 49.0000.2400.0000.0011.00**	**redistribute connected**
router-6(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-6(config-router)# **is-type level-1**	**network 11.1.1.0 0.0.0.255 area 0**
router-6(config-router)# **mpls traffic-eng level-1**	**network 24.1.1.1 0.0.0.0 area 0**
router-6(config-router)# **passive-interface Loopback0**	**network 12.1.1.0 0.0.0.255 area 0**
router-6(config-router)#	**network 13.1.1.0 0.0.0.255 area 0**
router-6(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-6(config-router)# mpls traffic-eng router-id Loopback0
router-6(config-router)# exit
```

Create a virtual interface:

```
router-6(config)# interface Loopback0
router-6(config-if)# ip address 25.1.1.1 255.255.255.255
router-6(config-if)# exit
At the device level, to coordinate traffic across the router and switch portions of the
device:
router-6(config)# interface atm9/0 0/0/0
router-6(config-if)# label-control-protocol vsi
router-6(config-if)# exit
router-6(config)# mpls traffic-eng atm cos sub-pool
router-6(config)# mpls traffic-eng atm cos global-pool premiun
```

For one incoming network interface:

```
router-6(config)# interface Xtagatm22

router-6(config-if)# extended-port atm9/0 bpx2.2
router-6(config-if)# ip address 10.1.1.2 255.0.0.0
router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-6(config-if)# mpls traffic-eng tunnels
router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
[and in either case]:
router-6(config-if)# exit
```

For the other incoming network interface: router-6(config)# **interface xtagatm55**

```
router-6(config-if)# extended-port atm9/0 bpx5.5
router-6(config-if)# ip address 11.1.1.2 255.0.0.0
router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-6(config-if)# mpls traffic-eng tunnels
router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
[and in either case]:
router-6(config-if)# exit
```

For one outgoing network interface: router-6(config)# **interface Xtagatm33**

```
router-6(config-if)# extended-port atm9/0 bpx3.3
router-6(config-if)# ip address 11.1.1.2 255.0.0.0
router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-6(config-if)# mpls traffic-eng tunnels
router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
[and in either case]:
router-6(config-if)# exit
```

For the other outgoing network interface: router-6(config)# **interface Xtagatm44**

```
router-6(config-if)# extended-port atm9/0 bpx4.4
router-6(config-if)# ip address 12.1.1.1 255.0.0.0
router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-6(config-if)# mpls traffic-eng tunnels
router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
[and in either case]:
router-6(config-if)# exit
```

Tunnel Midpoint Configuration LC-ATM Ingress

This 7200 midpoint router sits at the right-side edge of the MPLS ATM cloud in Figure 7. Therefore its ingress interface is LC-ATM and its egress can be either POS or ACM-PVC.

Configuring the Pools and Tunnels

At the device level:

```
router-8(config)# ip cef
router-8(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-8(config)# **router isis**	**router ospf 100**
router-8(config-router)# **net 49.2500.1000.0000.0012.00**	**redistribute connected**
router-8(config-router)# **metric-style wide**	**network 13.1.1.0 0.0.0.255 area 0**
router-8(config-router)# **is-type level-1**	**network 14.1.1.0 0.0.0.255 area 0**
router-8(config-router)# **mpls traffic-eng level-1**	**network 25.1.1.1 0.0.0.0 area 0**
router-8(config-router)# **passive-interface Loopback0**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-8(config-router)# mpls traffic-eng router-id Loopback0
router-8(config-router)# exit
```

Create a virtual interface:

```
router-8(config)# interface Loopback0
router-8(config-if)# ip address 27.1.1.1 255.255.255.255
router-8(config-if)# exit
```

At the incoming network interface level:

```
router-8(config)# interface atm8/2
router-8(config-if)# mpls traffic-eng tunnels
router-8(config-if)# ip rsvp bandwidth 140000 140000\ sub-pool 60000
router-8(config-if)# interface atm8/2.0 mpls
router-8(config-subif)# ip address 13.1.1.2 255.0.0.0
router-8(config-subif)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-8(config-subif)# mpls traffic-eng tunnels
router-8(config-subif)# mpls atm vpi 2-15
[if using IS-IS instead of OSPF]:
router-8(config-subif)# ip router isis
router-8(config-subif)# exit
```

And in all cases:

```
router-8(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-8(config)# **interface atm6/1**	**interface POS3/1**

[then continue each case at the network interface level]:

router-8(config-if)# **mpls traffic-eng tunnels**	**ip address 14.1.1.1 255.0.0.0**
router-8(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-8(config-if)# **interface atm6/1.3**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-8(config-subif)# **ip address 14.1.1.1 255.0.0.0**	
router-8(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-8(config-subif)# **mpls traffic-eng tunnels**	
router-8(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-8(config-subif)# **ip router isis**	
router-8(config-subif)# **exit**	
router-8(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-8(config-if)# exit
```

Tunnel Tail Configuration

The inbound interfaces on the 7200 tail router are configured identically to the inbound interfaces of the midpoint routers (except, of course, for the ID of each particular interface):

Configuring the Pools and Tunnels

At the device level:

```
router-4-8-or-7(config)# ip cef
router-4-8-or-7(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

`router-4-8-or-7(config)# router isis`	`router ospf 100`
`router-4-8-or-7(config-router)# net 49.0000.2700.0000.0000.00`	`redistribute connected`
`router-4-8-or-7(config-router)# metric-style wide`	`network 12.1.1.0 0.0.0.255 area 0`
`router-4-8-or-7(config-router)# is-type level-1`	`network 14.1.1.0 0.0.0.255 area 0`
`router-4-8-or-7(config-router)# mpls traffic-eng level-1`	`network 27.1.1.1 0.0.0.0 area 0`
`router-4-8-or-7(config-router)# passive-interface Loopback0`	`mpls traffic-eng area 0`

[now one resumes the common command set]:

```
router-4-8-or-7(config-router)# mpls traffic-eng router-id Loopback0
router-4-8-or-7(config-router)# exit
```

Create a virtual interface:

```
router-4-8-or-7(config)# interface Loopback0
router-4-8-or-7(config-if)# ip address 27.1.1.1 255.255.255.255
[but on router-7 in Figure 7 use ip address 28.1.1.1 255.255.255.255
]
router-4-8-or-7(config-if)# exit
```

For the incoming network interface, first at the device level:

[LC-ATM case appears on the left; POS case on the right]:

`router-4-8-or-7(config)# interface atm8/1`	`interface POS2/1`

[then continue each case at the network interface level]:

router-4-8-or-7(config-if)# **mpls traffic-eng tunnels**	**ip address 12.1.1.2 255.0.0.0**
router-4-8-or-7(config-if)# **ip rsvp bandwidth 140000\ 140000 sub-pool 60000**	**mpls traffic-eng tunnels**
router-4-8-or-7(config-if)# **interface atm8/1.2 mpls**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-4-8-or-7(config-subif)# **ip address 12.1.1.2 255.0.0.0**	
router-4-8-or-7(config-subif)#**ip rsvp bandwidth 140000\ 140000 sub-pool 60000**	
router-4-8-or-7(config-subif)# **mpls traffic-eng tunnels**	
router-4-8-or-7(config-subif)# **mpls atm vpi 2-5**	
[if using IS-IS instead of OSPF]:	
router-4-8-or-7(config-subif)# **ip router isis**	
router-4-8-or-7(config-subif)# **exit**	
router-4-8-or-7(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-4-8-or-7(config-if)# exit
```

Because the tunnel ends on the tail (does not include any outbound interfaces of the tail router), no outbound QoS configuration is used.

Example with Many Destination Prefixes

The two figures below illustrate topologies for guaranteed bandwidth services whose destinations are a set of prefixes. In the first figure below the interfaces to be configured are POS (Packet over SONET), while in second figure below the interfaces are ATM-PVC (Asynchronous Transfer Mode – Permanent Virtual Circuit). In both illustrations, the destinations' prefixes usually share some common properties such as belonging to the same Autonomous System (AS) or transiting through the same AS. Although the individual prefixes may change dynamically because of route flaps in the downstream autonomous systems, the properties the prefixes share will not change. Policies addressing the destination prefix set are enforced through Border Gateway Protocol (BGP), which is described in the following documents:

- "Configuring QoS Policy Propagation via Border Gateway Protocol" in the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.1 (http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt1/qcdprop.htm)
- "Configuring BGP" in the *Cisco IOS IP and IP Routing Configuration Guide,* Release 12.1 (http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdbgp.htm)
- "BGP Commands" in the *Cisco IOS IP and IP Routing Command Reference,* Release 12.1 (http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/1rdbgp.htm)

In this example, three guaranteed bandwidth services are offeref:

- Traffic coming from Site A (defined as all traffic arriving at interface FE4/0) and from Site C (defined as all traffic arriving at interface FE2/1) destined to AS5
- Traffic coming from Sites A and C that transits AS5 but is not destined to AS5. (In the figure, the transiting traffic will go to AS6 and AS7)

- Traffic coming from Sites A and C destined to prefixes advertised with a particular BGP community attribute (100:1). In this example, Autonomous Systems #3, #5, and #8 are the BGP community assigned the attribute 100:1.

Figure 32: Sample Topology for Guaranteed Bandwidth Service (traversing POS interfaces) to Many Destination Prefixes

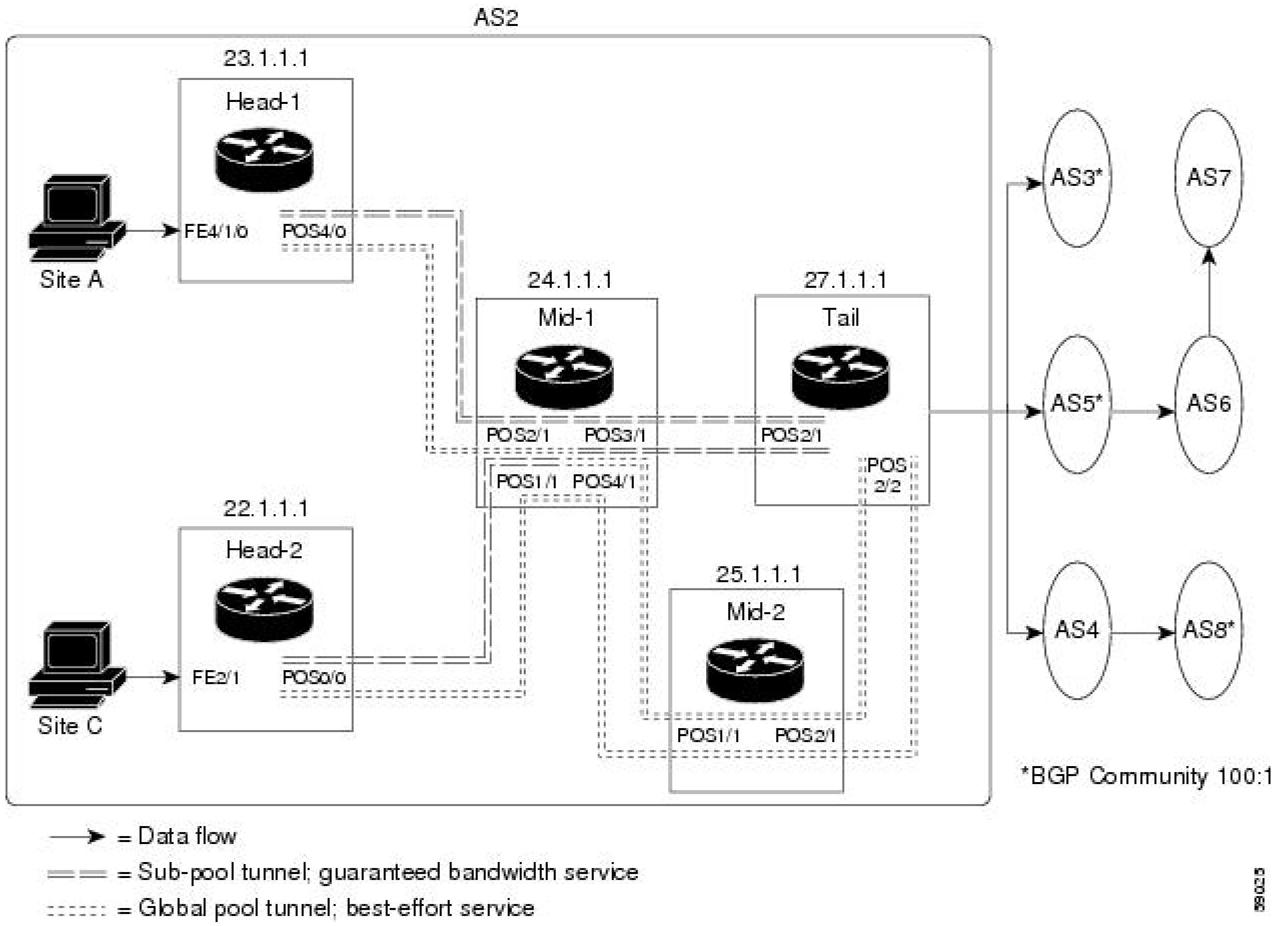
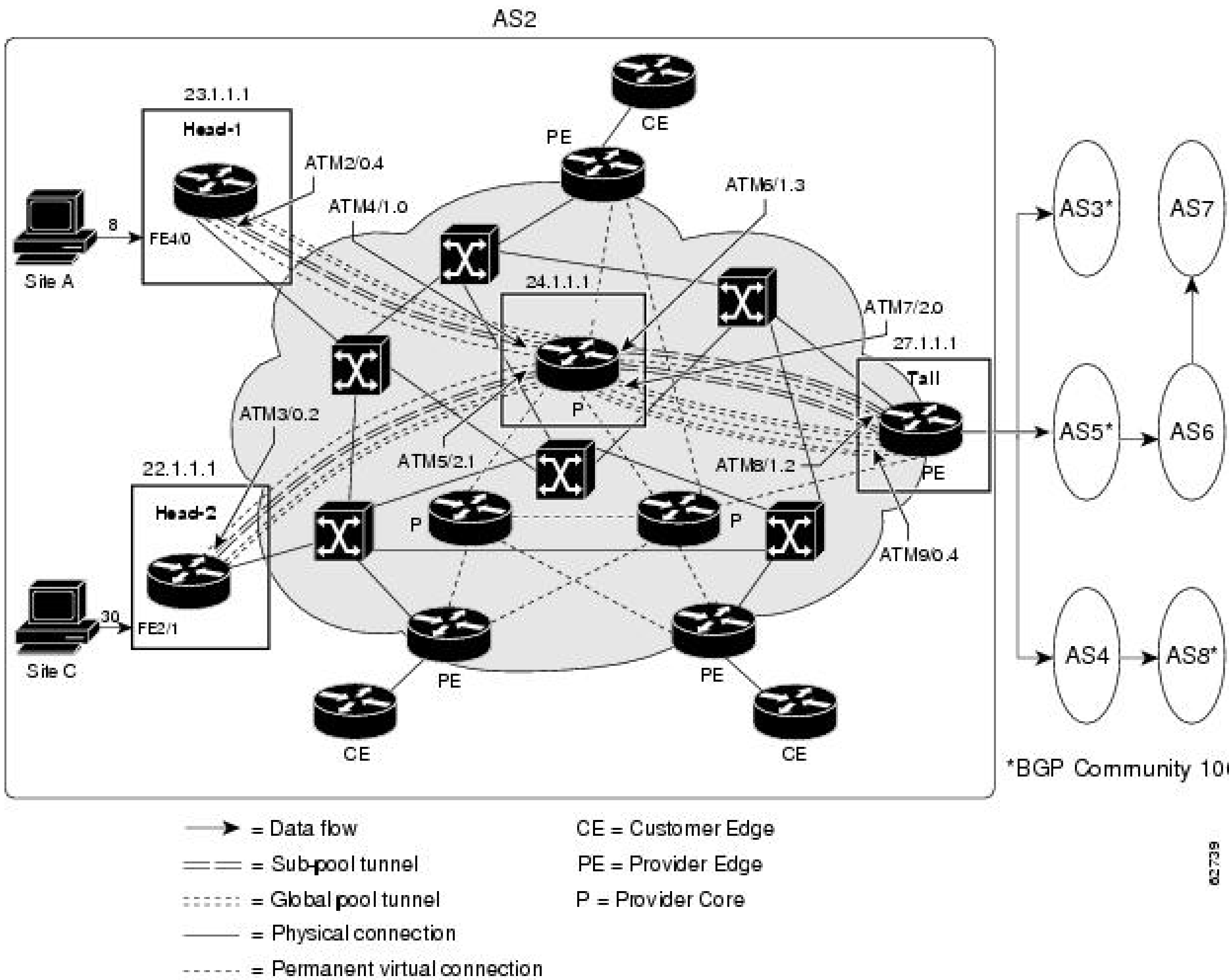


Figure 33: Sample Topology for Guaranteed Bandwidth Service (traversing ATM-PVC interfaces) to Many Destination Prefixes



The applicability of guaranteed bandwidth service is not limited to the three types of multiple destination scenarios described above. There is not room in this document to present all possible scenarios. These three were chosen as representative of the wide range of possible deployments.

The guaranteed bandwidth services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the tail
- From the Head-2 router, 22.1.1.1, to that same tail

In addition, a global pool tunnel has been configured from each head end, to carry best-effort traffic to the same destinations. All four tunnels use the same tail router, even though they have different heads and differ in their passage through the midpoint(s). (Of course in the real world there would likely be many more midpoints than just the one or two shown here.)

All POS and ATM-PVC interfaces in this example are OC3, whose capacity is 155 Mbps.

Configuring a multi-destination guaranteed bandwidth service involves:

- Building a sub-pool MPLS-TE tunnel
- Configuring DiffServ QoS

- Configuring QoS Policy Propagation via BGP (QPPB)
- Mapping traffic onto the tunnels

All of these tasks are included in the following example.

Tunnel Head Configuration Head-1

First we recapitulate commands that establish a sub-pool tunnel (commands presented earlier on page 9) and now we also configure a global pool tunnel. Additionally, we present QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (With the 7200 router, Modular QoS CLI is used).

Configuring the Pools and Tunnels

At the device level:

```
router-1(config)# ip cef
router-1(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# **router isis**	**router ospf 100**
router-1(config-router)# **net 49.0000.1000.0000.0010.00**	**redistribute connected**
router-1(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-1(config-router)# **is-type level-1**	**network 23.1.1.1 0.0.0.0 area 0**
router-1(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
```

Create a virtual interface:

```
router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-1(config)# **interface atm2/0**	**interface POS4/0**

[then continue each case at the network interface level:

router-1(config-if)# **mpls traffic-eng tunnels**	**ip address 10.1.1.1 255.0.0.0**
router-1(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-1(config-if)# **interface atm2/0.4**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-1(config-subif)# **ip address 10.1.1.1 0.0.0.0**	
router-1(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-1(config-subif)# **mpls traffic-eng tunnels**	
router-1(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-1(config-subif)# **ip router isis**	
router-1(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-1(config)# interface Tunnel1
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path1
router-1(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-1(config)# interface Tunnel2
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
```

```
router-1(config-if)# tunnel mpls traffic-eng bandwidth 80000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \ best-effort-path1
router-1(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-1(config)# ip explicit-path name gbs-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
router-1(config)# ip explicit-path name best-effort-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 25.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

Configuring DiffServ QoS

At the inbound network interface (in Figure 8 and Figure 9 this is FE4/0), packets received are rate-limited to:

- a rate of 30 Mbps
- a normal burst of 1 MB
- a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are droppef:

```
router-1(config)# interface FastEthernet4/0
router-1(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
 conform-action set-mpls-exp-transmit 5 exceed-action drop
router-1(config-if)# bgp-policy destination ip-qos-map
router-1(config-if)# exit
```

At the device level create a class of traffic called "exp5-class" that has MPLS experimental bit set to 5:

```
router-1(config)# class-map match-all exp5-class
router-1(config-cmap)# match mpls experimental 5
router-1(config-cmap)# exit
```

Create a policy that creates a priority queue for "exp5-class":

```
router-1(config)# policy-map core-out-policy
router-1(config-pmap)# class exp5-class
router-1(config-pmap-c)# priority 100000
router-1(config-pmap-c)# exit
router-1(config-pmap)# class class-default
router-1(config-pmap-c)# bandwidth 55000
router-1(config-pmap-c)# exit
router-1(config-pmap)# exit
```

The policy is applied to packets exiting subinterface ATM2/0.4 (first example) or interface POS4/0 (second example)?:

```
interface atm2/0
```

```
interface atm2/0.4
service-policy output core-out-policy

interface POS4/0
service-policy output\ core-out-policy
```

Configuring QoS Policy Propagation via BGP

For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-1(config)# router bgp 2
router-1(config-router)# no synchronization
router-1(config-router)# table-map set-qos-group
router-1(config-router)# bgp log-neighbor-changes
router-1(config-router)# neighbor 27.1.1.1 remote-as 2
router-1(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-1(config-router)# no auto-summary
router-1(config-router)# exit
```

For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 (a virtual loopback configured in the tail router; see page 57) so they will be mapped onto Tunnel #1 (the guaranteed bandwidth service tunnel). At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 100
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 100 permit ^5$
```

For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 101
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 101 permit _5_
```

For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match community 20
router-1(config-route-map)# set ip qos-group 6
```

```
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip community-list 20 permit 100:1
```

Mapping Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #1:

```
router-1(config)# ip route 29.1.1.1 255.255.255.255 Tunnel1
```

Map all best-effort traffic (traveling toward another virtual loopback interface, 30.1.1.1, configured in the tail router) onto Tunnel #2:

```
router-1(config)# ip route 30.1.1.1 255.255.255.255 Tunnel2
```

Tunnel Head Configuration Head-2

As with the Head-1 device and interfaces, the following Head-2 configuration first presents commands that establish a sub-pool tunnel (commands presented earlier on page 9) and then also configures a global pool tunnel. After that it presents QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (Because this is a 7200 router, Modular QoS CLI is used).

Configuring the Pools and Tunnels

At the device level:

```
router-2(config)# ip cef
router-2(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# **router isis**	**router ospf 100**
router-2(config-router)# **net 49.0000.1000.0000.0011.00**	**redistribute connected**
router-2(config-router)# **metric-style wide**	**network 11.1.1.0 0.0.0.255 area 0**
router-2(config-router)# **is-type level-1**	**network 22.1.1.1 0.0.0.0 area 0**
router-2(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
```

```
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-2(config)# **interface atm3/0**	**interface POS0/0**

[then continue each case at the network interface level:

router-2(config-if)# **mpls traffic-eng tunnels**	**ip address 11.1.1.1 255.0.0.0**
router-2(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-2(config-if)# **interface atm3/0.2**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-2(config-subif)# **ip address 11.1.1.1 255.0.0.0**	
router-2(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-2(config-subif)# **mpls traffic-eng tunnels**	
router-2(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-2(config-subif)# **ip router isis**	
router-2(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-2(config-if)# ip router isis
[and in all cases]:
router-2(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-2(config)# interface Tunnel3
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
```

```
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path2
router-2(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-2(config)# interface Tunnel4
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth 70000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \ best-effort-path2
router-2(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-2(config)# ip explicit-path name gbs-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
router-2(config)# ip explicit-path name best-effort-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 25.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

Configuring DiffServ QoS

At the inbound network interface (in Figure 8 and Figure 9 this is FE2/1), packets received are rate-limited to:

- a rate of 30 Mbps
- a normal burst of 1 MB
- a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are droppef:

```
router-2(config)# interface FastEthernet2/1
router-2(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
 conform-action set-mpls-exp-transmit 5 exceed-action drop
router-2(config-if)# bgp-policy destination ip-qos-map
router-2(config-if)# exit
```

At the device level create a class of traffic called "exp5-class" that has MPLS experimental bit set to 5:

```
router-2(config)# class-map match-all exp5-class
router-2(config-cmap)# match mpls experimental 5
router-2(config-cmap)# exit
```

Create a policy that creates a priority queue for "exp5-class":

```
router-2(config)# policy-map core-out-policy
router-2(config-pmap)# class exp5-class
router-2(config-pmap-c)# priority 100000
```

```
router-2(config-pmap-c)# exit
router-2(config-pmap)# class class-default
router-2(config-pmap-c)# bandwidth 55000
router-2(config-pmap-c)# exit
router-2(config-pmap)# exit
```

The policy is applied to packets exiting subinterface ATM3/0.2 (left side) or interface POS0/0 (right side):

interface atm3/0	interface POS0/0
interface atm3/0.2	service-policy output\ core-out-policy
service-policy output core-out-policy	

Configuring QoS Policy Propagation via BGP

For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-2(config)# router bgp 2
router-2(config-router)# no synchronization
router-2(config-router)# table-map set-qos-group
router-2(config-router)# bgp log-neighbor-changes
router-2(config-router)# neighbor 27.1.1.1 remote-as 2
router-2(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-2(config-router)# no auto-summary
router-2(config-router)# exit
```

For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 (a virtual loopback configured in the tail router; see page 57) so they will be mapped onto Tunnel #3 (th e guaranteed bandwidth service tunnel). At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 100
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 100 permit ^5$
```

For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 101
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
```

```
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 101 permit _5_
```

For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match community 20
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip community-list 20 permit 100:1
```

Mapping Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #3:

```
router-2(config)# ip route 29.1.1.1 255.255.255.255 Tunnel3
```

Map all best-effort traffic onto Tunnel #4 (traveling toward another virtual loopback interface, 30.1.1.1, configured in the tail router):

```
router-2(config)# ip route 30.1.1.1 255.255.255.255 Tunnel4
```

Tunnel Midpoint Configuration Mid-1

All four interfaces on the midpoint router are configured very much like the outbound interface of the head router. The strategy is to have all mid-point routers in this Autonomous System ready to carry future as well as presently configured sub-pool and global pool tunnels.

Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-3(config)# **router isis**	**router ospf 100**
router-3(config-router)# **net 49.0000.2400.0000.0011.00**	**redistribute connected**
router-3(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-3(config-router)# **is-type level-1**	**network 11.1.1.0 0.0.0.255 area 0**
router-3(config-router)# **mpls traffic-eng level-1**	**network 24.1.1.1 0.0.0.0 area 0**
router-3(config-router)#	**network 12.1.1.0 0.0.0.255 area 0**
router-3(config-router)#	**network 13.1.1.0 0.0.0.255 area 0**
router-3(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit
```

Create a virtual interface:

```
router-3(config)# interface Loopback0
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# exit
```

At one incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm4/1**	**interface POS2/1**

[then continue each case at the network interface level:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 10.1.1.2 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 70000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm4/1.0**	**ip rsvp bandwidth 140000 140000\ sub-pool 70000**
router-3(config-subif)# **ip address 10.1.1.2 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 70000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

At the other incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm5/2**	**interface POS1/1**

[then continue each case at the network interface level:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 11.1.1.2 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 70000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm5/2.1**	**ip rsvp bandwidth 140000 140000\ sub-pool 70000**
router-3(config-subif)# **ip address 11.1.1.2 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 70000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

At the outgoing network interface through which two sub-pool tunnels currently exit:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm6/1**	**interface POS3/1**

[then continue each case at the network interface level:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 12.1.1.1 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 70000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm6/1.3**	**ip rsvp bandwidth 140000 140000\ sub-pool 70000**
router-3(config-subif)# **ip address 12.1.1.1 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 70000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

At the outgoing network interface through which two global pool tunnels currently exit:

[ATM-PVC case appears on the left; POS case on the right]:

router-3(config)# **interface atm7/2**	**interface POS4/1**

[then continue each case at the network interface level:

router-3(config-if)# **mpls traffic-eng tunnels**	**ip address 13.1.1.1 255.0.0.0**
router-3(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 70000**	**mpls traffic-eng tunnels**
router-3(config-if)# **interface atm7/2.0**	**ip rsvp bandwidth 140000 140000\ sub-pool 70000**
router-3(config-subif)# **ip address 13.1.1.1 255.0.0.0**	
router-3(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 70000**	
router-3(config-subif)# **mpls traffic-eng tunnels**	
router-3(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-3(config-subif)# **ip router isis**	
router-3(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

Tunnel Midpoint Configuration Mid-2

[For the sake of simplicity, only the POS example (Figure 8) is illustrated with a second midpoint router.] Both interfaces on this midpoint router are configured like the outbound interfaces of the Mid-1 router.

Configuring the Pools and Tunnels

At the device level:

```
router-5(config)# ip cef
router-5(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-5(config)# **router isis**	**router ospf 100**
router-5(config-router)# **net 49.2500.1000.0000.0012.00**	**redistribute connected**
router-5(config-router)# **metric-style wide**	**network 13.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **is-type level-1**	**network 14.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **mpls traffic-eng level-1**	**network 25.1.1.1 0.0.0.0 area 0**
router-5(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit
```

Create a virtual interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit
```

At the incoming network interface:

```
router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

At the outgoing network interface:

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

Tunnel Tail Configuration

The inbound interfaces on the tail router are configured much like the outbound interfaces of the midpoint routers:

Configuring the Pools and Tunnels

At the device level:

```
router-4(config)# ip cef
router-4(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right. In the case of OSPF, one must advertise two new loopback interfaces--29.1.1.1 and 30.1.1.1 in our example--which are defined in the QoS Policy Propagation section, further along on this page]:

router-4(config)# **router isis**	**router ospf 100**
router-4(config-router)# **net 49.0000.2700.0000.0000.00**	**redistribute connected**
router-4(config-router)# **metric-style wide**	**network 12.1.1.0 0.0.0.255 area 0**
router-4(config-router)# **is-type level-1**	**network 14.1.1.0 0.0.0.255 area 0**
router-4(config-router)# **mpls traffic-eng level-1**	**network 27.1.1.1 0.0.0.0 area 0**
router-4(config-router)#	**network 29.1.1.1 0.0.0.0 area 0**
router-4(config-router)#	**network 30.1.1.1 0.0.0.0 area 0**
router-4(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set, taking care to include the two additional loopback interfaces]:

```
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# mpls traffic-eng router-id Loopback1
router-4(config-router)# mpls traffic-eng router-id Loopback2
router-4(config-router)# exit
```

Create a virtual interface:

```
router-4(config)# interface Loopback0
router-4(config-if)# ip address 27.1.1.1 255.255.255.255
router-4(config-if)# exit
```

At one incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-4(config)# **interface atm8/1**	**interface POS2/1**

[then continue each case at the network interface level:

router-4(config-if)# **mpls traffic-eng tunnels**	**ip address 12.1.1.2 255.0.0.0**
router-4(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 70000**	**mpls traffic-eng tunnels**
router-4(config-if)# **interface atm8/1.2**	**ip rsvp bandwidth 140000 140000\ sub-pool 70000**
router-4(config-subif)# **ip address 12.1.1.2 255.0.0.0**	
router-4(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 70000**	
router-4(config-subif)# **mpls traffic-eng tunnels**	
router-4(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-4(config-subif)# **ip router isis**	
router-4(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit
```

At the other incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-4(config)# **interface atm8/1**	**interface POS2/2**

[then continue each case at the network interface level:

router-4(config-if)# **mpls traffic-eng tunnels**	**ip address 14.1.1.2 255.0.0.0**
router-4(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 70000**	**mpls traffic-eng tunnels**
router-4(config-if)# **interface atm8/1.2**	**ip rsvp bandwidth 140000 140000\ sub-pool 70000**
router-4(config-subif)# **ip address 14.1.1.2 255.0.0.0**	
router-4(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 70000**	
router-4(config-subif)# **mpls traffic-eng tunnels**	
router-4(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-4(config-subif)# **ip router isis**	
router-4(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type: [If using IS-IS instead of OSPF]:

```
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit
```

Configuring QoS Policy Propagation

On the tail device, one must configure a separate virtual loopback IP address for each class-of-service terminating here. The headend routers need these addresses to map traffic into the proper tunnels. In the current example, four tunnels terminate on the same tail device but they represent only two service classes, so only two additional loopback addresses are needef:

Create two virtual interfaces:

```
router-4(config)# interface Loopback1
router-4(config-if)# ip address 29.1.1.1 255.255.255.255
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
```

```
router-4(config-if)# exit
router-4(config)# interface Loopback2
router-4(config-if)# ip address 30.1.1.1 255.255.255.255
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit
```

At the device level, configure BGP to send the community to each tunnel heaf:

```
router-4(config)# router bgp 2
router-4(config-router)# neighbor 23.1.1.1 send-community
router-4(config-router)# neighbor 22.1.1.1 send-community
router-4(config-router)# exit
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Asynchronous Transfer Mode Command Reference*. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List*.

- **debug mpls traffic-engineering link-management preemption**
- **extended-port**
- **interface**
- **ip cef**
- **ip router isis**
- **ip rsvp bandwidth**
- **is-type**
- **metric-style wide**
- **mpls traffic-eng**
- **mpls traffic-eng administrative-weight**
- **mpls traffic-eng area**
- **mpls traffic-eng atm cos global-pool**
- **mpls traffic-eng atm cos sub-pool**
- **mpls traffic-eng attribute-flags**
- **mpls traffic-eng backup-path tunnel**
- **mpls traffic-eng flooding thresholds**
- **mpls traffic-eng link timers bandwidth-hold**
- **mpls traffic-eng link timers periodic-flooding**
- **mpls traffic-eng reoptimize timers frequency**
- **mpls traffic-eng router-id**
- **mpls traffic-eng tunnels (configuration)**

- **mpls traffic-eng tunnels (interface)**
- **net**
- **passive-interface**
- **router isis**
- **router ospf**
- **show interfaces tunnel**
- **show ip ospf**
- **show ip route**
- **show ip rsvp host**
- **show ip rsvp interface**
- **show mpls traffic-eng autoroute**
- **show mpls traffic-eng fast-reroute database**
- **show mpls traffic-eng fast-reroute log reroutes**
- **show mpls traffic-eng link-management admission-control**
- **show mpls traffic-eng link-management advertisements**
- **show mpls traffic-eng link-management bandwidth-allocation**
- **show mpls traffic-eng link-management igp-neighbors**
- **show mpls traffic-eng link-management interfaces**
- **show mpls traffic-eng link-management summary**
- **show mpls traffic-eng topology**
- **show mpls traffic-eng tunnels**
- **mpls atm vpi**
- **tunnel destination**
- **tunnel mode mpls traffic-eng**
- **tunnel mpls traffic-eng affinity**
- **tunnel mpls traffic-eng autoroute announce**
- **tunnel mpls traffic-eng autoroute metric**
- **tunnel mpls traffic-eng bandwidth**
- **tunnel mpls traffic-eng fast-reroute**
- **tunnel mpls traffic-eng path-option**
- **tunnel mpls traffic-eng priority**

Glossary

customer edge (CE) router --A router that belongs to a customer network, which connects to a provider edge (PE) router to utilize Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) network services.

provider edge (PE) router --Entry point into the service provider network. The PE router is typically deployed on the edge of the network and is administered by the service provider. The PE router is the redistribution point between Enhanced Interior Gateway Routing Protocol (EIGRP) and Border Gateway Protocol (BGP) in PE to CE networking.

pseudowire (PW)--A mechanism that carries the elements of an emulated service from one provider edge (PE) to one or more PEs over a packet-switched network (PSN).

VPN --virtual private network. Allows IP traffic to travel securely over public TCP/IP networks and the Internet by encapsulating and encrypting all IP packets. VPN uses a tunnel to encrypt all information at the IP level.

Note Refer to Internetworking Terms and Acronyms for terms not included in this glossary.

CHAPTER 20

End of Life for LAN Emulation

Support for LAN emulation (LANE) feature and commands has been removed in Cisco IOS Release 15.1M and later releases. This change marks the end of life for LAN emulation.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Removal of Support for LAN Emulation Feature

The following LAN Emulation feature is obsolete and is no longer available from Cisco IOS Release 15.1M and later releases:

- LAN Emulation Overview
- Configuring LAN Emulation
- Configuring Token Ring LAN Emulation
- Configuring Token Ring LAN Emulation for Multiprotocol over ATM

Removal of Support for LAN Emulation Commands

The following commands are obsolete and are no longer available from Cisco IOS Release 15.1M and later releases (no replacement commands are provided):

- **debug atm bus**
- **debug lane client**
- **debug lane config**
- **debug lane finder**
- **debug lane server**
- **debug lane signaling**
- **lane auto-config-atm-address**
- **lane bus-atm-address**
- **lane client**
- **lane client-atm-address**
- **lane client flush**
- **lane client mpoa client name**
- **lane client mpoa server name**
- **lane config-atm-address**
- **lane config database**
- **lane database**
- **lane fixed-config-atm-address**
- **lane fssrp**
- **lane global-lecs-address**
- **lane le-arp**
- **lane server-atm-address**
- **lane server-bus**
- **show lane**
- **show lane bus**
- **show lane client**
- **show lane config**
- **show lane database**
- **show lane default-atm-addresses**
- **show lane le-arp**

- **show lane neighbor**
- **show lane qos database**
- **show lane server**

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List
ATM commands	Asynchronous Transfer Mode Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for End of Life for LAN Emulation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 21: Feature Information for End of Life for LAN Emulation

Feature Name	Releases	Feature Information
End of Life for LAN Emulation	15.1M	Support for LAN emulation has been removed from the Cisco IOS software.

CHAPTER 21

LAN Emulation Overview

This overview chapter gives a high-level description of LAN Emulation (LANE).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

LAN Emulation

The Cisco implementation of LANE makes an ATM interface look like one or more Ethernet interfaces.

LANE is an ATM service defined by the ATM Forum specification LAN Emulation over ATM, ATM_FORUM 94-0035. This service emulates the following LAN-specific characteristics:

- Connectionless services
- Multicast services
- LAN MAC driver services

LANE service provides connectivity between ATM-attached devices and connectivity with LAN-attached devices. This includes connectivity between ATM-attached stations and LAN-attached stations and also connectivity between LAN-attached stations across an ATM network.

Because LANE connectivity is defined at the MAC layer, upper protocol-layer functions of LAN applications can continue unchanged when the devices join emulated LANs (ELANs). This feature protects corporate investments in legacy LAN applications.

An ATM network can support multiple independent ELAN networks. Membership of an end system in any of the ELANs is independent of the physical location of the end system. This characteristic enables easy hardware moves and location changes. In addition, the end systems can also move easily from one ELAN to another, whether or not the hardware moves.

LANE in an ATM environment provides routing between ELANs for supported routing protocols and high-speed, scalable switching of local traffic.

The ATM LANE system has three servers that are single points of failure. These are the LANE Configuration Server (LECS), the ELAN server (LES), and the broadcast and unknown server (BUS). Beginning with Cisco IOS Release 11.2, LANE fault tolerance or Simple LANE Service Replication on the ELAN provides backup servers to prevent problems if these servers fail.

The fault tolerance mechanism that eliminates these single points of failure is described in the "Configuring LAN Emulation" chapter. Although this scheme is proprietary, no new protocol additions have been made to the LANE subsystems.

LANE Components

Any number of ELANs can be set up in an ATM switch cloud. A router can participate in any number of these ELANs.

LANE is defined on a LAN client/server model. The following components are implemented:

- LANE client--A LANE client emulates a LAN interface to higher layer protocols and applications. It forwards data to other LANE components and performs LANE address resolution functions.

Each LANE client is a member of only one ELAN. However, a router can include LANE clients for multiple ELANs: one LANE client for *each* ELAN of which it is a member.

If a router has clients for multiple ELANs, the Cisco IOS software can route traffic between the ELANs.

- LES--The LES for an ELAN is the control center. It provides joining, address resolution, and address registration services to the LANE clients in that ELAN. Clients can register destination unicast and multicast MAC addresses with the LES. The LES also handles LANE ARP (LE ARP) requests and responses.

The Cisco implementation has a limit of one LES per ELAN.

- LANE BUS--The LANE BUS sequences and distributes multicast and broadcast packets and handles unicast flooding.

In this release, the LES and the LANE BUS are combined and located in the same Cisco 7000 family or Cisco 4500 series router; one combined LECS and BUS is required per ELAN.

- LECS--The LECS contains the database that determines which ELAN a device belongs to (each configuration server can have a different named database). Each LANE client consults the LECS just once, when it joins an ELAN, to determine which ELAN it should join. The LECS returns the ATM address of the LES for that ELAN.

One LECS is required per LANE ATM switch cloud.

The LECS's database can have the following four types of entries:

- • ELAN name-ATM address of LES pairs

- LANE client MAC address-ELAN name pairs
- LANE client ATM template-ELAN name pairs
- Default ELAN name

Note ELAN names must be unique on an interface. If two interfaces participate in LANE, the second interface may be in a different switch cloud.

LANE Operation and Communication

Communication among LANE components is ordinarily handled by several types of switched virtual circuits (SVCs). Some SVCs are unidirectional; others are bidirectional. Some are point-to-point and others are point-to-multipoint. The figure below illustrates the various virtual channel connections (VCCs)--also known as virtual circuit connections--that are used in LANE configuration.

The figure below shows LANE components: LE server stands for the LANE server (LECS), *LECS* stands for the LANE configuration server, and *BUS* stands for the LANE broadcast.

Figure 34: LANE VCC Types

The following section describes various processes that occur, starting with a client requesting to join an ELAN after the component routers have been configured.

Client Joining an ELAN

The following process normally occurs after a LANE client has been enabled:

- Client requests to join an ELAN--The client sets up a connection to the LECS--a bidirectional point-to-point Configure Direct VCC--to find the ATM address of the LES for its ELAN.

LANE clients find the LECS by using the following methods in the listed order:

-
    - Locally configured ATM address
    - Interim Local Management Interface (ILMI)
    - Fixed address defined by the ATM Forum
    - PVC 0/17

- Configuration server identifies the LES--Using the same VCC, the LECS returns the ATM address and the name of the LES for the client's ELAN.
- Client contacts the server for its LAN--The client sets up a connection to the LES for its ELAN (a bidirectional point-to-point Control Direct VCC) to exchange control traffic.

Once a Control Direct VCC is established between a LANE client and a LES, it remains up.

- Server verifies that the client is allowed to join the ELAN--The server for the ELAN sets up a connection to the LECS to verify that the client is allowed to join the ELAN--a bidirectional point-to-point Configure

Direct (server) VCC. The server's configuration request contains the client's MAC address, its ATM address, and the name of the ELAN. The LECS checks its database to determine whether the client can join that LAN; then it uses the same VCC to inform the server whether the client is or is not allowed to join.

- LES allows or disallows the client to join the ELAN--If allowed, the LES adds the LANE client to the unidirectional point-to-multipoint Control Distribute VCC and confirms the join over the bidirectional point-to-point Control Direct VCC. If disallowed, the LES rejects the join over the bidirectional point-to-point Control Direct VCC.
- LANE client sends LE ARP packets for the broadcast address, which is all **1**s--Sending LE ARP packets for the broadcast address sets up the VCCs to and from the BUS.

Address Resolution

As communication occurs on the ELAN, each client dynamically builds a local LANE ARP (LE ARP) table. A LE ARP table belonging to a client can also have static, preconfigured entries. The LE ARP table maps MAC addresses to ATM addresses.

Note LE ARP is not the same as IP ARP. IP ARP maps IP addresses (Layer 3) to Ethernet MAC addresses (Layer 2); LE ARP maps ELAN MAC addresses (Layer 2) to ATM addresses (also Layer 2).

When a client first joins an ELAN, its LE ARP table has no dynamic entries and the client has no information about destinations on or behind its ELAN. To learn about a destination when a packet is to be sent, the client begins the following process to find the ATM address corresponding to the known MAC address:

- The client sends a LE ARP request to the LES for this ELAN (point-to-point Control Direct VCC).
- The LES forwards the LE ARP request to all clients on the ELAN (point-to-multipoint Control Distribute VCC).
- Any client that recognizes the MAC address responds with its ATM address (point-to-point Control Direct VCC).
- The LES forwards the response (point-to-multipoint Control Distribute VCC).
- The client adds the MAC address-ATM address pair to its LE ARP cache.
- Then the client can establish a VCC to the desired destination and send packets to that ATM address (bidirectional point-to-point Data Direct VCC).

For unknown destinations, the client sends a packet to the BUS, which forwards the packet to all clients via flooding. The BUS floods the packet because the destination might be behind a bridge that has not yet learned this particular address.

Multicast Traffic

When a LANE client has broadcast or multicast traffic, or unicast traffic with an unknown address to send, the following process occurs:

- The client sends the packet to the BUS (unidirectional point-to-point Multicast Send VCC).

- The BUS forwards (floods) the packet to all clients (unidirectional point-to-multipoint Multicast Forward VCC).

This VCC branches at each ATM switch. The switch forwards such packets to multiple outputs. (The switch does not examine the MAC addresses; it simply forwards all packets it receives.)

Typical LANE Scenarios

In typical LANE cases, one or more Cisco 7000 family routers, or Cisco 4500 series routers are attached to a Cisco LightStream ATM switch. The LightStream ATM switch provides connectivity to the broader ATM network switch cloud. The routers are configured to support one or more ELANs. One of the routers is configured to perform the LECS functions. A router is configured to perform the server function and the BUS function for each ELAN. (One router can perform the server function and the BUS function for several ELANs.) In addition to these functions, each router also acts as a LANE client for one or more ELANs.

This section presents two scenarios using the same four Cisco routers and the same Cisco LightStream ATM switch. The figure in the "Single ELAN Scenario" section show one ELAN set up on the switch and routers. The figure in the "Multiple ELAN Scenario" section shows several ELANs set up on the switch and routers.

The physical layout and the physical components of an emulated network might not differ for the single and the multiple ELAN cases. The differences are in the software configuration for the number of ELANs and the assignment of LANE components to the different physical components.

Single ELAN Scenario

In a single ELAN scenario, the LANE components might be assigned as follows:

- Router 1 includes the following LANE components:
    - The LECS (one per LANE switch cloud)
    - The LES and BUS for the ELAN with the default name *man* (for Manufacturing)
    - The LANE client for the *man* ELAN.
- Router 2 includes a LANE client for the *man* ELAN.
- Router 3 includes a LANE client for the *man* ELAN.
- Router 4 includes a LANE client for the *man* ELAN.

The figure below illustrates this single ELAN configured across several routers.

Figure 35: Single ELAN Configured on Several Routers

Multiple ELAN Scenario

In the multiple LAN scenario, the same switch and routers are used, but multiple ELANs are configured. See the figure below.

Figure 36: Multiple ELANs Configured on Several Routers

In the following scenario, three ELANs are configured on four routers:

- Router 1 includes following LANE components:
  - The LECS (one per LANE switch cloud)
  - The LES and BUS for the ELAN called *man* (for Manufacturing)
  - The LES and BUS functions for the ELAN called *eng* (for Engineering)
  - A LANE client for the *man* ELAN
  - A LANE client for the *eng* ELAN
- Router 2 includes only the LANE clients for the *man* and *eng* ELANs.
- Router 3 includes only the LANE clients for the *man* and *mkt* (for Marketing) ELANs.
- Router 4 includes the following LANE components:
  - The LES and BUS for the *mkt* ELAN
  - A LANE client for the *man* ELAN
  - A LANE client for the *mkt* ELANs

In this scenario, once routing is enabled and network level addresses are assigned, Router 1 and Router 2 can route between the *man* and the *eng* ELANs, and Router 3 and Router 4 can route between the *man* and the *mkt* ELANs.

CHAPTER 22

Configuring LAN Emulation

This chapter describes how to configure LAN emulation (LANE) on the following platforms that are connected to an ATM switch or switch cloud:

- ATM Interface Processor (AIP) on the Cisco 7500 series routers
- ATM port adapter on the Cisco 7200 series and Cisco 7500 series routers
- Network Processor Module (NPM) on the Cisco 4500 and Cisco 4700 routers

Note Beginning with Cisco IOS Release 11.3, all commands supported on the Cisco 7500 series routers are also supported on the Cisco 7000 series.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

LANE on ATM

LANE emulates an IEEE 802.3 Ethernet or IEEE 802.5 Token Ring LAN using ATM technology. LANE provides a service interface for network-layer protocols that is identical to existing MAC layers. No changes are required to existing upper layer protocols and applications. With LANE, Ethernet and Token Ring packets are encapsulated in the appropriate ATM cells and sent across the ATM network. When the packets reach the other side of the ATM network, they are deencapsulated. LANE essentially bridges LAN traffic across ATM switches.

Benefits of LANE

ATM is a cell-switching and multiplexing technology designed to combine the benefits of circuit switching (constant transmission delay and guaranteed capacity) with those of packet switching (flexibility and efficiency for intermittent traffic).

LANE allows legacy Ethernet and Token Ring LAN users to take advantage of ATM's benefits without modifying end-station hardware or software. ATM uses connection-oriented service with point-to-point signalling or multicast signalling between source and destination devices. However, LANs use connectionless service. Messages are broadcast to all devices on the network. With LANE, routers and switches emulate the connectionless service of a LAN for the endstations.

By using LANE, you can scale your networks to larger sizes while preserving your investment in LAN technology.

LANE Components

A single emulated LAN (ELAN) consists of the following entities: A LECS, a BUS, a LES, and LANE clients.

- LANE configuration server--A server that assigns individual clients to particular emulated LANs by directing them to the LES for the ELAN. The LANE configuration server (LECS) maintains a database of LANE client and server ATM or MAC addresses and their emulated LANs. An LECS can serve multiple emulated LANs.
- LANE broadcast and unknown server--A multicast server that floods unknown destination traffic and forwards multicast and broadcast traffic to clients within an ELAN. One broadcast and unknown server (BUS) exists per ELAN.
- LANE server--A server that provides a registration facility for clients to join the ELAN. There is one LANE server (LES) per ELAN. The LES handles LAN Emulation Address Resolution Protocol (LE ARP) requests and maintains a list of LAN destination MAC addresses. For Token Ring LANE, the LES also maintains a list of route-descriptors that is used to support source-route bridging (SRB) over the ELAN. The route-descriptors are used to determine the ATM address of the next hop in the Routing Information Field (RIF).
- LANE client--An entity in an endpoint, such as a router, that performs data forwarding, address resolution, and other control functions for a single endpoint in a single ELAN. The LANE client (LEC) provides standard LAN service to any higher layers that interface with it. A router can have multiple resident LANE clients, each connecting with different emulated LANs. The LANE client registers its MAC and ATM addresses with the LES.

ELAN entities coexist on one or more Cisco routers. On Cisco routers, the LES and the BUS are combined into a single entity.

Other LANE components include ATM switches--any ATM switch that supports the Interim Local Management Interface (ILMI) and signalling. Multiple emulated LANs can coexist on a single ATM network.

Simple Server Redundancy

LANE relies on three servers: the LECS, the LES, and the BUS. If any one of these servers fails, the ELAN cannot fully function.

Cisco has developed a fault tolerance mechanism known as simple server redundancy that eliminates these single points of failure. Although this scheme is proprietary, no new protocol additions have been made to the LANE subsystems.

Simple server redundancy uses multiple LECSs and multiple broadcast-and-unknown and LESs. You can configure servers as backup servers, which will become active if a master server fails. The priority levels for the servers determine which servers have precedence.

Refer to the "Configuring Fault-Tolerant Operation" section for details and notes on the Simple Server Redundancy Protocol (SSRP).

LANE Implementation Considerations

Network Support

In this release, Cisco supports the following networking features:

- Ethernet-emulated LANs
  - Routing from one ELAN to another via IP, IPX, or AppleTalk
  - Bridging between emulated LANs and between emulated LANs and other LANs
  - DECnet, Banyan VINES, and XNS routed protocols
- Token-Ring emulated LANs
  - IP routing (fast switched) between emulated LANs and between a Token Ring ELAN and a legacy LAN
  - IPX routing between emulated LANs and between a Token Ring ELAN and a legacy LAN
  - Two-port and multiport SRB (fast switched) between emulated LANs and between emulated LANs and a Token Ring
  - IP and IPX multiring
  - SRB, source-route translational bridging (SR/TLB), and source-route transparent bridging (SRT)
  - AppleTalk for (IOS) TR-LANE and includes Appletalk fast switched routing.
  - DECnet, Banyan VINES, and XNS protocols are not supported

Cisco's implementation of LAN Emulation over 802.5 uses existing terminology and configuration options for Token Rings, including SRB. For more information about configuring SRB, see the chapter "Configuring Source-Route Bridging" in the Cisco IOS Bridging and IBM Networking Configuration Guide. Transparent bridging and Advanced Peer-to-Peer Networking (APPN) are not supported at this time.

- Hot Standby Router Protocol (HSRP)

For information about configuring APPN over Ethernet LANE, refer to the "Configuring APPN" chapter in the Cisco IOS Bridging and IBM Networking Configuration Guide.

Hardware Support

This release of LANE is supported on the following platforms:

- Cisco 4500-M, Cisco 4700-M
- Cisco 7200 series
- Cisco 7500 series

Note Beginning with Cisco IOS Release 11.3, all commands supported on the Cisco 7500 series routers are also supported on the Cisco 7000 series routers equipped with RSP7000. Token Ring LAN emulation on Cisco 7000 series routers requires the RSP7000 upgrade. The RSP7000 upgrade requires a minimum of 24 MB DRAM and 8 MB Flash memory.

The router must contain an ATM Interface Processor (AIP), ATM port adapter, or an NP-1A ATM Network Processor Module (NPM). These modules provide an ATM network interface for the routers. Network interfaces reside on modular interface processors, which provide a direct connection between the high-speed Cisco Extended Bus (CxBus) and the external networks. The maximum number of AIPs, ATM port adapters, or NPMs that the router supports depends on the bandwidth configured. The total bandwidth through all the AIPs, ATM port adapters, or NPMs in the system should be limited to 200 Mbps full duplex--two Transparent Asynchronous Transmitter/Receiver Interfaces (TAXIs), one Synchronous Optical Network (SONET) and one E3, or one SONET and one lightly used SONET.

This feature also requires one of the following switches:

- Cisco LightStream 1010 (recommended)
- Cisco LightStream 100
- Any ATM switch with UNI 3.0/3.1 and ILMI support for communicating the LECS address

TR-LANE requires Cisco IOS Release 3.1(2) or later on the LightStream 100 switch and Cisco IOS Release 11.1(8) or later on the LightStream 1010.

For a complete description of the routers, switches, and interfaces, refer to your hardware documentation.

Addressing

On a LAN, packets are addressed by the MAC-layer address of the destination and source stations. To provide similar functionality for LANE, MAC-layer addressing must be supported. Every LANE client must have a

MAC address. In addition, every LANE component (server, client, BUS, and LECS) must have an ATM address that is different from that of all the other components.

All LANE clients on the same interface have the same, automatically assigned MAC address. That MAC address is also used as the end-system identifier (ESI) part of the ATM address, as explained in the next section. Although client MAC addresses are not unique, all ATM addresses are unique.

LANE ATM Addresses

A LANE ATM address has the same syntax as an NSAP, but it is not a network-level address. It consists of the following:

- A 13-byte prefix that includes the following fields defined by the ATM Forum:
    - AFI (Authority and Format Identifier) field (1 byte)
    - DCC (Data Country Code) or ICD (International Code Designator) field (2 bytes)
    - DFI field (Domain Specific Part Format Identifier) (1 byte)
    - Administrative Authority field (3 bytes)
    - Reserved field (2 bytes)
    - Routing Domain field (2 bytes)
    - Area field (2 bytes)
- A 6-byte end-system identifier (ESI)
- A 1-byte selector field

Method of Automatically Assigning ATM Addresses

We provide the following standard method of constructing and assigning ATM and MAC addresses for use in a LECS's database. A pool of MAC addresses is assigned to each ATM interface on the router. On the Cisco 7200 series routers, Cisco 7500 series routers, Cisco 4500 routers, and Cisco 4700 routers, the pool contains eight MAC addresses. For constructing ATM addresses, the following assignments are made to the LANE components:

- The prefix fields are the same for all LANE components in the router; the prefix indicates the identity of the switch. The prefix value must be configured on the switch.
- The ESI field value assigned to every *client* on the interface is the first of the pool of MAC addresses assigned to the interface.
- The ESI field value assigned to every *server* on the interface is the second of the pool of MAC addresses.
- The ESI field value assigned to the *broadcast-and-unknown serve* r on the interface is the third of the pool of MAC addresses.
- The ESI field value assigned to the *configuration server* is the fourth of the pool of MAC addresses.
- The selector field value is set to the subinterface number of the LANE component--except for the LECS, which has a selector field value of 0.

Because the LANE components are defined on different subinterfaces of an ATM interface, the value of the selector field in an ATM address is different for each component. The result is a unique ATM address for each LANE component, even within the same router. For more information about assigning components to subinterfaces, see the "Rules for Assigning Components to Interfaces and Subinterfaces, on page 553" section later in this chapter.

For example, if the MAC addresses assigned to an interface are 0800.200C.1000 through 0800.200C.1007, the ESI part of the ATM addresses is assigned to LANE components as follows:

- Any client gets the ESI 0800.200c.1000.
- Any server gets the ESI 0800.200c.1001.
- The BUS gets the ESI 0800.200c.1002.
- The LECS gets the ESI 0800.200c.1003.

Refer to the "Multiple Token Ring ELANs with Unrestricted Membership Example, on page 578" and the "Multiple Token Ring ELANs with Restricted Membership Example, on page 580" sections for examples using MAC address values as ESI field values in ATM addresses and for examples using subinterface numbers as selector field values in ATM addresses.

Using ATM Address Templates

ATM address templates can be used in many LANE commands that assign ATM addresses to LANE components (thus overriding automatically assigned ATM addresses) or that link client ATM addresses to emulated LANs. The use of templates can greatly simplify the use of these commands. The syntax of address templates, the use of address templates, and the use of wildcard characters within an address template for LANE are very similar to those for address templates of ISO CLNS.

Note E.164-format ATM addresses do not support the use of LANE ATM address templates.

LANE ATM address templates can use two types of wildcards: an asterisk (*) to match any single character, and an ellipsis (...) to match any number of leading or trailing characters.

In LANE, a *prefix template* explicitly matches the prefix but uses wildcards for the ESI and selector fields. An *ESI template* explicitly matches the ESI field but uses wildcards for the prefix and selector. The table below indicates how the values of unspecified digits are determined when an ATM address template is used:

Table 22: Values of Unspecified Digits in ATM Address Templates

Unspecified Digits In	Value Is
Prefix (first 13 bytes)	Obtained from ATM switch via Interim Local Management Interface (ILMI)

Unspecified Digits In	Value Is
ESI (next 6 bytes)	Filled with the slot MAC address[24] plus • 0--LANE client • 1--LES • 2--LANE BUS • 3--LECS
Selector field (last 1 byte)	Subinterface number, in the range 0 through 255.

24 The lowest of the pool of MAC addresses assigned to the ATM interface plus a value that indicates the LANE component. For the Cisco 7200 series routers, Cisco 7500 series routers, Cisco 4500 routers, and Cisco 4700 routers, the pool has eight MAC addresses.

Rules for Assigning Components to Interfaces and Subinterfaces

The following rules apply to assigning LANE components to the major ATM interface and its subinterfaces in a given router:

- The LECS always runs on the major interface.

The assignment of any other component to the major interface is identical to assigning that component to the 0 subinterface.

- The server and the client of the *same* ELAN can be configured on the same subinterface in a router.
- Clients of two *different* emulated LANs cannot be configured on the same subinterface in a router.
- Servers of two *different* emulated LANs cannot be configured on the same subinterface in a router.

LANE Configuration Task List

Before you begin to configure LANE, you must decide whether you want to set up one or multiple emulated LANs. If you set up multiple emulated LANs, you must also decide where the servers and clients will be located, and whether to restrict the clients that can belong to each ELAN. Bridged emulated LANs are configured just like any other LAN, in terms of commands and outputs. Once you have made those basic decisions, you can proceed to configure LANE.

Once LANE is configured, you can configure Multiprotocol over ATM (MPOA). For MPOA to work with LANE, a LANE client must have an ELAN ID to work properly, a LANE client must have an ELAN ID. To set up a LANE client for MPOA and give an ELAN ID perform the tasks described in the following section:

- Setting Up LANE Clients for MPOA, on page 568

Although the sections described contain information about configuring SSRP fault tolerance, refer to the Configuring Fault-Tolerant Operation, on page 569 section for detailed information about requirements and implementation considerations.

Once LANE is configured, you can monitor and maintain the components in the participating routers by completing the tasks described in the Monitoring and Maintaining the LANE Components, on page 573 section.

For configuration examples, see the "LANE Configuration Examples, on page 576" section at the end of this chapter.

Creating a LANE Plan and Worksheet

Draw up a plan and a worksheet for your own LANE scenario, showing the following information and leaving space for noting the ATM address of each of the LANE components on each subinterface of each participating router:

- The router and interface where the LECS will be located.
- The router, interface, and subinterface where the LES and BUS for each ELAN will be located. There can be multiple servers for each ELAN for fault-tolerant operation.
- The routers, interfaces, and subinterfaces where the clients for each ELAN will be located.
- The name of the default ELAN (optional).
- The names of the emulated LANs that will have unrestricted membership.
- The names of the emulated LANs that will have restricted membership.

The last three items in this list are very important; they determine how you set up each ELAN in the LECS's database.

Configuring the Prefix on the Switch

Before you configure LANE components on any Cisco 7200 series router, Cisco 7500 series router, Cisco 4500 router, or Cisco 4700 router, you must configure the Cisco ATM switch with the ATM address prefix to be used by all LANE components in the switch cloud. On the Cisco switch, the ATM address prefix is called the node ID. Prefixes must be 26 digits long. If you provide fewer than 26 digits, zeros are added to the right of the specified value to fill it to 26 digits.

On the switches, you can display the current prefix by using the **show network** EXEC command.

Note If you do not save the configured value permanently, it will be lost when the switch is reset or powered off.

To set the ATM address prefix on the Cisco LightStream 1010 or on the Cisco LightStream 100 switch, follow these steps:

SUMMARY STEPS

1. Router(config)# **atm-address**{*atm-address* | *prefix*...}
2. Router(config)# **exit**
3. Router# **copy system:running-config nvram:startup-config**
4. Router(config-route-map)# **set local***nameip-address mask prefix*
5. Router(config-route-map)# **save**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **atm-address**{*atm-address* | *prefix*...}	(Cisco LightStream 1010 Switch) Sets the local node ID (prefix of the ATM address).
Step 2	Router(config)# **exit**	(Cisco LightStream 1010 Switch) Exits global configuration mode.
Step 3	Router# **copy system:running-config nvram:startup-config**	(Cisco LightStream 1010 Switch) Saves the configuration values permanently.
Step 4	Router(config-route-map)# **set local***nameip-address mask prefix*	(Cisco LightStream 100) Sets the local node ID (prefix of the ATM address).
Step 5	Router(config-route-map)# **save**	(Cisco LightStream 100) Saves the configuration values permanently.

Setting Up the Signalling and ILMI PVCs

You must set up the signalling permanent virtual circuit (PVC) and the PVC that will communicate with the ILMI on the major ATM interface of any router that participates in LANE.

Complete this task only once for a major interface. You do not need to repeat this task on the same interface even though you might configure LESs and clients on several of its subinterfaces.

To set up these PVCs, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1.
2. Router(config-if)# **atm pvc***vcd vpi vci* **qsaal**
3. Router(config-if)# **atm pvc***vcd vpi vci* **ilmi**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Example:** `Router(config-if)#` **interface atm** *slot*/**0** **Example:** `Router(config-if)#` **interface atm** *slot*/*port-adapter*/**0** **Example:** `Router(config-if)#` **interface atm** *number*	Specifies the major ATM interface and enter interface configuration mode: • On the AIP for Cisco 7500 series routers; on the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
Step 2	Router(config-if)# **atm pvc***vcd vpi vci* **qsaal**	Sets up the signalling PVC that sets up and tears down switched virtual circuits (SVCs); the *vpi* and *vci* values are usually set to 0 and 5, respectively.
Step 3	Router(config-if)# **atm pvc***vcd vpi vci* **ilmi**	Sets up a PVC to communicate with the ILMI; the *vpi* and *vci* values are usually set to 0 and 16, respectively.

Displaying LANE Default Addresses

You can display the LANE default addresses to make configuration easier. Complete this task for each router that participates in LANE. This command displays default addresses for all ATM interfaces present on the router. Write down the displayed addresses on your worksheet.

To display the default LANE addresses, use the following command in EXEC mode:

Command	Purpose
`Router#` **show lane default-atm-addresses**	Displays the LANE default addresses.

Entering the LECS ATM Address on the Cisco Switch

You must enter the LECS's ATM address into the Cisco LightStream 100 or Cisco Lightstream 1010 ATM switch and save it permanently so that the value is not lost when the switch is reset or powered off.

You must specify the full 40-digit ATM address. Use the addresses on your worksheet that you obtained from the previous task.

If you are configuring SSRP or Fast Simple Server Redundancy Protocol (FSSRP), enter the multiple LECS addresses into the end ATM switches. The switches are used as central locations for the list of LECS addresses. LANE components connected to the switches obtain the global list of LECS addresses from the switches.

Entering the ATM Addresses on the LightStream 1010 ATM Switch

On the Cisco LightStream 1010 ATM switch, the LECS address can be specified for a port or for the entire switch.

To enter the LECS addresses on the Cisco LightStream 1010 ATM switch for the entire switch, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **atm lecs-address-default***lecsaddress* [*sequence #*][25]
2. Router(config)# **exit**
3. Router# **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **atm lecs-address-default***lecsaddress* [*sequence #*][25]	Specifies the LECS's ATM address for the entire switch. If you are configuring SSRP, include the ATM addresses of all the LECSs.
Step 2	Router(config)# **exit**	Exits global configuration mode.
Step 3	Router# **copy system:running-config nvram:startup-config**	Saves the configuration value permanently.

25 Refer to the LightStream 1010 ATM Switch Command Reference for further information about this command.

Entering the ATM Addresses on the LightStream 1010 ATM Switch Per Port

To enter the LECS addresses on the Cisco LightStream 1010 ATM switch per port, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **atm lecs-address***lecsaddress* [*sequence #*][26]
2. Router(config-if)# **Ctrl-Z**
3. Router# **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **atm lecs-address***lecsaddress* [*sequence #*][26]	Specifies the LECS's ATM address for a port. If you are configuring SSRP, include the ATM addresses of all the LECSs.
Step 2	Router(config-if)# **Ctrl-Z**	Exits interface configuration mode.
Step 3	Router# **copy system:running-config nvram:startup-config**	Saves the configuration value permanently.

26 Refer to the LightStream 1010 ATM Switch Command Reference for further information about this command.

Entering the ATM Addresses on the Cisco LightStream 100 ATM Switch

To enter the LECS's ATM address into the Cisco LightStream 100 ATM switch and save it permanently, use the following commands in privileged EXEC mode:

SUMMARY STEPS

1. Router# **set configserver** index *atm-address*
2. Router# **save**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **set configserver** index *atm-address*	Specifies the LECS's ATM address. If you are configuring SSRP, repeat this command for each LECS address. The index value determines the priority. The highest priority is 0. There can be a maximum of 4 LECSs.
Step 2	Router# **save**	Saves the configuration value permanently.

Setting Up the LECS Database

The LECS's database contains information about each ELAN, including the ATM addresses of the LESs.

You can specify one default ELAN in the database. The LECS will assign any client that does not request a specific ELAN to the default ELAN.

Emulated LANs are either restricted or unrestricted. The LECS will assign a client to an unrestricted ELAN if the client specifies that particular ELAN in its configuration. However, the LECS will only assign a client to a restricted ELAN if the client is specified in the database of the LECS as belonging to that ELAN. The default ELAN must have unrestricted membership.

If you are configuring fault tolerance, you can have any number of servers per ELAN. Priority is determined by entry order; the first entry has the highest priority, unless you override it with the index option.

Setting Up the Database for the Default ELAN Only

When you configure a router as the LECS for one default ELAN, you provide a name for the database, the ATM address of the LES for the ELAN, and a default name for the ELAN. In addition, you indicate that the LECS's ATM address is to be computed automatically.

When you configure a database with only a default unrestricted ELAN, you do not have to specify where the LANE clients are located. That is, when you set up the LECS's database for a single default ELAN, you do not have to provide any database entries that link the ATM addresses of any clients with the ELAN name. All of the clients will be assigned to the default ELAN.

You can have any number of servers per ELAN for fault tolerance. Priority is determined by entry order. The first entry has the highest priority unless you override it with the index option.

If you are setting up only a default ELAN, the *elan-name* value in Steps 2 and 3 is the same as the default ELAN name you provide in Step 4.

To set up fault-tolerant operation, see the "Configuring Fault-Tolerant Operation, on page 569" section later in this chapter.

To set up the LECS for the default ELAN, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **lane database***database-name*
2. Router(lane-config-dat)# **name***elan-name***server-atm-address***atm-address* [**index** *number*]
3. Router(lane-config-dat)# **name***elan-name***local-seg-id***segment-number*
4. Router(lane-config-dat)# **default-name***elan-name*
5. Router(lane-config-dat)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **lane database***database-name*	Creates a named database for the LECS.
Step 2	Router(lane-config-dat)# **name***elan-name***server-atm-address***atm-address* [**index** *number*]	In the configuration database, binds the name of the ELAN to the ATM address of the LES. If you are configuring SSRP, repeat this step for each additional server for the same ELAN. The index determines the priority. The highest priority is 0.

	Command or Action	Purpose
Step 3	Router(lane-config-dat)# **name***elan-name***local-seg-id***segment-number*	If you are configuring a Token Ring ELAN, assigns a segment number to the emulated Token Ring LAN in the configuration database.
Step 4	Router(lane-config-dat)# **default-name***elan-name*	In the configuration database, provides a default name for the ELAN.
Step 5	Router(lane-config-dat)# **exit**	Exits from database configuration mode and return to global configuration mode.

Setting Up the Database for Unrestricted-Membership Emulated LANs

When you set up a database for unrestricted emulated LANs, you create database entries that link the name of each ELAN to the ATM address of its server.

However, you may choose not to specify where the LANE clients are located. That is, when you set up the LECS's database, you do not have to provide any database entries that link the ATM addresses or MAC addresses of any clients with the ELAN name. The LECS will assign the clients to the emulated LANs specified in the client's configurations.

To set up fault-tolerant operation, see the "Configuring Fault-Tolerant Operation, on page 569" section later in this chapter.

To configure a router as the LECS for multiple emulated LANs with unrestricted membership, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **lane database***database-name*
2. Router(lane-config-dat)# **name***elan-name1***server-atm-address***atm-address* [**index** *number*]
3. Router(lane-config-dat)# **name***elan-name2***server-atm-address***atm-address* [**index** *number*]
4. Router(lane-config-dat)# **name***elan -name1***local-seg-id***segment-number*
5. Router(lane-config-dat)# **name***elan -name2***local-seg-id***segment-number*
6. Router(lane-config-dat)# **default-name***elan-name1*
7. Router(lane-config-dat)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **lane database***database-name*	Creates a named database for the LECS.
Step 2	Router(lane-config-dat)# **name***elan-name1***server-atm-address***atm-address* [**index** *number*]	In the configuration database, binds the name of the first ELAN to the ATM address of the LES for that ELAN.

	Command or Action	Purpose
		If you are configuring SSRP, repeat this step with the same ELAN name but with different server ATM addresses for each additional server for the same ELAN. The index determines the priority. The highest priority is 0.
Step 3	Router(lane-config-dat)# **name***elan-name2***server-atm-address***atm-address* [**index** *number*]	In the configuration database, binds the name of the second ELAN to the ATM address of the LES. If you are configuring SSRP, repeat this step with the same ELAN name but with different server ATM addresses for each additional server for the same ELAN. The index determines the priority. The highest priority is 0. Repeat this step, providing a different ELAN name and ATM address for each additional ELAN in this switch cloud.
Step 4	Router(lane-config-dat)# **name***elan -name1***local-seg-id***segment-number*	For a Token Ring ELAN, assigns a segment number to the first emulated Token Ring LAN in the configuration database.
Step 5	Router(lane-config-dat)# **name***elan -name2***local-seg-id***segment-number*	For Token Ring emulated LANs, assigns a segment number to the second emulated Token Ring LAN in the configuration database. Repeat this step, providing a different ELAN name and segment number for each additional source-route bridged ELAN in this switch cloud.
Step 6	Router(lane-config-dat)# **default-name***elan-name1*	(Optional) Specifies a default ELAN for LANE clients not explicitly bound to an ELAN.
Step 7	Router(lane-config-dat)# **exit**	Exits from database configuration mode and return to global configuration mode.

Setting Up the Database for Restricted-Membership LANs

When you set up the database for restricted-membership emulated LANs, you create database entries that link the name of each ELAN to the ATM address of its server.

However, you must also specify where the LANE clients are located. That is, for each restricted-membership ELAN, you provide a database entry that explicitly links the ATM address or MAC address of each client of that ELAN with the name of that ELAN.

The client database entries specify which clients are allowed to join the ELAN. When a client requests to join an ELAN, the LECS consults its database and then assigns the client to the ELAN specified in the LECS's database.

When clients for the same restricted-membership ELAN are located in multiple routers, each client's ATM address or MAC address must be linked explicitly with the name of the ELAN. As a result, you must configure as many client entries (at Steps 6 and 7, in the following procedure) as you have clients for emulated LANs in all the routers. Each client will have a different ATM address in the database entries.

To set up fault-tolerant operation, see the "Configuring Fault-Tolerant Operation, on page 569" section later in this chapter.

To set up the LECS for emulated LANs with restricted membership, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **lane database***database-name*
2. Router(lane-config-dat)# **name***elan-name1***server-atm-address***atm-address* **restricted** [**index** *number*]
3. Router(lane-config-dat)# **name***elan-name2***server-atm-address***atm-address* **restricted** [**index** *number*]
4. Router(lane-config-dat)# **name***elan -name1***local-seg-id***segment-number*
5. Router(lane-config-dat)# **name***elan -name2***local-seg-id***segment-number*
6. Router(lane-config-dat)# **client-atm-address***atm-address-template***name***elan-name1*
7. Router(lane-config-dat)# **client-atm-address***atm-address-template***name***elan-name2*
8. Router(lane-config-dat)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **lane database***database-name*	Creates a named database for the LECS.
Step 2	Router(lane-config-dat)# **name***elan-name1***server-atm-address***atm-address* **restricted** [**index** *number*]	In the configuration database, binds the name of the first ELAN to the ATM address of the LES for that ELAN. If you are configuring SSRP, repeat this step with the same ELAN name but with different server ATM addresses for each additional server for the same ELAN. The index determines the priority. The highest priority is 0.
Step 3	Router(lane-config-dat)# **name***elan-name2***server-atm-address***atm-address* **restricted** [**index** *number*]	In the configuration database, binds the name of the second ELAN to the ATM address of the LES. If you are configuring SSRP, repeat this step with the same ELAN name but with different server ATM addresses for each additional server for the same ELAN. The index determines the priority. The highest priority is 0. Repeat this step, providing a different name and a different ATM address, for each additional ELAN.
Step 4	Router(lane-config-dat)# **name***elan -name1***local-seg-id***segment-number*	For a Token Ring ELAN, assigns a segment number to the first emulated Token Ring LAN in the configuration database.
Step 5	Router(lane-config-dat)# **name***elan -name2***local-seg-id***segment-number*	If you are configuring Token Ring emulated LANs, assigns a segment number to the second emulated Token Ring LAN in the configuration database. Repeat this step, providing a different ELAN name and segment number for each additional source-route bridged ELAN in this switch cloud.

	Command or Action	Purpose
Step 6	Router(lane-config-dat)# **client-atm-address***atm-address-template***name***elan-name1*	Adds a database entry associating a specific client's ATM address with the first restricted-membership ELAN. Repeat this step for each of the clients of the first restricted-membership ELAN.
Step 7	Router(lane-config-dat)# **client-atm-address***atm-address-template***name***elan-name2*	Adds a database entry associating a specific client's ATM address with the second restricted-membership ELAN. Repeat this step for each of the clients of the second restricted-membership ELAN. Repeat this step, providing a different name and a different list of client ATM address, for each additional ELAN.
Step 8	Router(lane-config-dat)# **exit**	Exits from database configuration mode and return to global configuration mode.

Enabling the LECS

Once you have created the database, you can enable the LECS on the selected ATM interface and router by using the following commands beginning in global configuration mode:

SUMMARY STEPS

1.
2. Router(config-if)# **lane config database***database-name*
3. Do one of the following:
    - Router(config-if)# **lane config auto-config-atm-address**
    - Router(config-if)# **lane config auto-config-atm-address**
    -
    - Router(config-if)# **lane config fixed-config-atm-address** Router(config-if)# **lane config fixed-config-atm-address**
4. **exit**
5. **Ctrl-Z**
6. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Example:** `Router(config)#` **interface atm** *slot*/**0**[*.subinterface-number* **Example:** `Router(config)#` **interface atm** *slot*/*port-adapter*/**0**[*.subinterface-number*] **Example:** `Router(config)#` **interface atm** *number* [*.subinterface-number*]	If you are not currently configuring the interface, specifies the major ATM interface where the LECS is located. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
Step 2	Router(config-if)# **lane config database***database-name*	Link the LECS's database name to the specified major interface, and enable the LECS.
Step 3	Do one of the following: • Router(config-if)# **lane config auto-config-atm-address** • Router(config-if)# **lane config auto-config-atm-address** • • Router(config-if)# **lane config fixed-config-atm-address** Router(config-if)# **lane config fixed-config-atm-address** **Example:** `Router(config-if)#` **lane config config-atm-address** *atm-address-template*	Specifies how the LECS's ATM address will be computed. You may opt to choose one of the following scenarios: The LECS will participate in SSRP and the address is computed by the automatic method. The LECS will participate in SSRP, and the address is computed by the automatic method. If the LECS is the master, the fixed address is also used. The LECS will not participate in SSRP, the LECS is the master, and only the well-known address is used. The LECS will participate in SSRP and the address is computed using an explicit, 20-byte ATM address.

	Command or Action	Purpose
Step 4	**exit**	Exits interface configuration mode.
Step 5	**Ctrl-Z**	Returns to EXEC mode.
Step 6	**copy system:running-config nvram:startup-config**	Saves the configuration.

Setting Up LESs and Clients

For each router that will participate in LANE, set up the necessary servers and clients for each ELAN; then display and record the server and client ATM addresses. Be sure to keep track of the router interface where the LECS will eventually be located.

You can set up servers for more than one ELAN on different subinterfaces or on the same interface of a router, or you can place the servers on different routers.

When you set up a server and BUS on a router, you can combine them with a client on the same subinterface, a client on a different subinterface, or no client at all on the router.

Where you put the clients is important because any router with clients for multiple emulated LANs can route frames between those emulated LANs.

Depending on where your clients and servers are located, perform one of the following tasks for each LANE subinterface.

Setting Up the Server and BUS and Client

If the ELAN in Step 3 is intended to have *restrictedmembership*, consider carefully whether you want to specify its name here. You will specify the name in the LECS's database when it is set up. However, if you link the client to an ELAN in this step, and through some mistake it does not match the database entry linking the client to an ELAN, this client will not be allowed to join this ELAN or any other.

If you do decide to include the name of the ELAN linked to the client in Step 3 and later want to associate that client with a different ELAN, make the change in the LECS's database before you make the change for the client on this subinterface.

Each ELAN is a separate subnetwork. In Step 4 make sure that the clients of the same ELAN are assigned protocol addresses on the same subnetwork and that clients of different emulated LANs are assigned protocol addresses on different subnetworks.

To set up the server, BUS, and (optionally) clients for an ELAN, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot* **/0**.*subinterface-number*
2. Router(config-if)# **lane server-bus**{**ethernet**| **tokenring**} *elan-name*
3. Router(config-if)# **lane client**{**ethernet**| **tokenring**} [*elan-name*] [**elan-id** *id*]
4. Router(config-if)# **ip***address mask*
5. Router(config-if)# **Ctrl-Z**
6. Router# **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot* **/0**.*subinterface-number* **Example:** `Router(config)#` **interface atm** *slot* **/** *port-adapter* **/0**`.subinterface-number` **Example:** `Router(config)#` **interface atm** *number* **.** *subinterface-number*	Specifies the subinterface for the ELAN on this router. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
Step 2	Router(config-if)# **lane server-bus**{**ethernet**| **tokenring**} *elan-name*	Enables a LES and a LANE BUS for the ELAN.
Step 3	Router(config-if)# **lane client**{**ethernet**| **tokenring**} [*elan-name*] [**elan-id** *id*]	(Optional) Enables a LANE client for the ELAN. To participate in MPOA, configures the LES and a LANE BUS for the ELAN with the ELAN ID.
Step 4	Router(config-if)# **ip***address mask*	Provides a protocol address for the client. • The command or commands depend on the routing protocol used. If you are using IPX or AppleTalk, see the relevant protocol chapter (IPX or AppleTalk) in the Cisco IOS AppleTalk and Novell IPX Configuration Guide for the commands to use.
Step 5	Router(config-if)# **Ctrl-Z**	Returns to EXEC mode.
Step 6	Router# **copy system:running-config nvram:startup-config**	Saves the configuration.

Setting Up Only a Client on a Subinterface

On any given router, you can set up one client for one ELAN or multiple clients for multiple emulated LANs. You can set up a client for a given ELAN on any routers you choose to participate in that ELAN. Any router with clients for multiple emulated LANs can route packets between those emulated LANs.

You must first set up the signalling and ILMI PVCs on the major ATM interface, as described earlier in the "Setting Up the Signalling and ILMI PVCs, on page 555" section, before you set up the client.

Each ELAN is a separate subnetwork. In Step 2, make sure that the clients of the same ELAN are assigned protocol addresses on the same subnetwork and that clients of different emulated LANs are assigned protocol addresses on different subnetworks.

To set up only a client for an emulated LANs, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot* **/0.** *subinterface-number*
2. Router(config-if)# **ip***address mask*
3. Router(config-if)# **lane client**{**ethernet**| **tokenring**} [*elan-name*]
4. Router(config-if)# **Ctrl-Z**
5. Router# **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot* **/0.** *subinterface-number* **Example:** `Router(config)#` **interface atm** *slot* / *port-adapter* **/0.** *subinterface-number* **Example:** `Router(config)#` **interface atm** *number* **.** *subinterface-number*	Specifies the subinterface for the ELAN on this router. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
Step 2	Router(config-if)# **ip***address mask*	Provides a protocol address for the client on this subinterface. • The command or commands depend on the routing protocol used. If you are using IPX or AppleTalk, see the relevant protocol chapter (IPX or AppleTalk) in the Cisco IOS AppleTalk and Novell IPX Configuration Guide for the commands to use.

	Command or Action	Purpose
Step 3	Router(config-if)# **lane client** {**ethernet**| **tokenring**} [*elan-name*]	Enables a LANE client for the ELAN.
Step 4	Router(config-if)# **Ctrl-Z**	Returns to EXEC mode.
Step 5	Router# **copy system:running-config nvram:startup-config**	Saves the configuration.

Disabling the FLUSH Process of LAN Emulation Clients

Disable the LE_FLUSH process and make the transition from using the BUS to using a data direct virtual channel connection (VCC). Disabling the LE_FLUSH process is recommended to prevent the initial packet drops during the establishment of LANE Direct VC. With the LE_FLUSH process disabled, LAN Emulation Clients (LECs) in the node will not send a flush request and will directly use a data direct VCC for data transfer.

Note Disabling the LE_FLUSH process affects all the LECs in a Cisco networking device.

To keep LECs from sending LE_FLUSH messages to the remote LEC, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **no lane client flush**	Disables the flush mechanism of a LEC.

Setting Up LANE Clients for MPOA

For Multiprotocol over ATM (MPOA) to work properly, a LANE client must have an ELAN ID for all ELANs represented by the LANE client.

Caution If an ELAN ID is supplied by both commands, make sure that the ELAN ID matches in both.

For more information on configuring the MPOA client, refer to the "Configuring the Multiprotocol over ATM Client " chapter.

To configure an ELAN ID, use one of the following commands in LANE database configuration mode or in interface configuration mode when starting up the LES for that ELAN:

Command	Purpose
Router(lane-config-dat)# **name** *elan-name* **elan-id** *id*	Configures the ELAN ID in the LAN Emulation Client Server (LECS) database to participate in MPOA.
Router(lane-config-dat)# **lane server-bus** {**ethernet** | **tokenring**} *elan-name* [**elan-id** *id*]	Configures the LES and a LANE BUS for the ELAN (ELAN). To participate in MPOA, configure the LES and a LANE BUS for the ELAN with the ELAN ID.

Configuring Fault-Tolerant Operation

The LANE simple server redundancy feature creates fault tolerance using standard LANE protocols and mechanisms. If a failure occurs on the LECS or on the LES/BUS, the ELAN can continue to operate using the services of a backup LES. This protocol is called the SSRP.

This section describes how to configure simple server redundancy for fault tolerance on an ELAN.

Note This server redundancy does not overcome other points of failure beyond the router ports: Additional redundancy on the LAN side or in the ATM switch cloud are not a part of the LANE simple server redundancy feature.

Simple Server Redundancy Requirements

For simple LANE service replication or fault tolerance to work, the ATM switch must support multiple LES addresses. This mechanism is specified in the LANE standard. The LE servers establish and maintain a standard control circuit that enables the server redundancy to operate.

LANE simple server redundancy is supported on Cisco IOS Release 11.2 and later. Older LANE configuration files continue to work with this new software.

This redundancy feature works only with Cisco LECSs and LES/BUS combinations. Third-party LANE Clients can be used with the SSRP, but third-party configuration servers, LE servers, and BUS do not support SSRP.

For server redundancy to work correctly:

- All the ATM switches must have identical lists of the global LECS addresses, in the identical priority order.
- The operating LECSs must use exactly the same configuration database. Load the configuration table data using the **copy rcp tftp**} system:**running-config** command. This method minimizes errors and enables the database to be maintained centrally in one place.

The LANE protocol does not specify where any of the ELAN server entities should be located, but for the purpose of reliability and performance, Cisco implements these server components on its routers.

Fast Simple Server Redundancy Requirements

Fast Simple Server Replication Protocol (FSSRP) differs from LANE SSRP in that all configured LE servers of an ELAN are always active. FSSRP-enabled LANE clients have virtual circuits (VCs) established to a maximum of four LE servers and broadcast and unknown servers (BUSs) at one time. If a single LES goes down, the LANE client quickly switches over to the next LES and BUS resulting in no data or LE-ARP table entry loss and no extraneous signalling.

Due to the increase in LAN client connections to all LE servers in an ELAN, FSSRP increases the number of VCs in your network. On a per client basis, up to 12 additional VCs will be added. These include the additional control direct, control distribute, multicast send and multicast forward VCs (times the 3 extra LE servers and BUSs), which totals 12 additional VCs.

Users should take care to calculate whether or not the number of existing VCs in their network can be maintained with additional VC connections to the secondary LE servers and BUSs.

A LANE client may connect to up to only 4 LE servers and BUSs at a time.

Redundant Configuration Servers

To enable redundant LECSs, enter the multiple LECS addresses into the end ATM switches. LANE components can obtain the list of LECS addresses from the ATM switches through the Interim Local Management Interface (ILMI).

Refer to the "Entering the LECS ATM Address on the Cisco Switch, on page 557" section for more details.

Redundant Servers and BUSs

The LECS turns on server/BUS redundancy by adjusting its database to accommodate multiple server ATM addresses for a particular ELAN. The additional servers serve as backup servers for that ELAN.

To activate the feature, you add an entry for the hierarchical list of servers that will support the given ELAN. All database modifications for the ELAN must be identical on all LECSs.

Refer to the "Setting Up the LECS Database, on page 558" section for more details.

Implementation Considerations

The following is a list of LANE implementation restrictions:

- The LightStream 1010 can handle up to 16 LECS addresses. The LightStream 100 allows a maximum of 4 LECS addresses.
- There is no limit on the number of LE servers that can be defined per ELAN.
- When a LECS switchover occurs, no previously joined clients are affected.
- When a LES/BUS switches over, momentary loss of clients occurs until they are all transferred to the new LES/BUS.
- LECSs come up as masters until a higher-level LECS tells them otherwise. This is automatic and cannot be changed.

- If a higher-priority LES comes online, it bumps the current LES off on the same ELAN. Therefore, there may be some flapping of clients from one LES to another after a powerup, depending on the order of the LE servers coming up. Flapping should settle after the last highest-priority LES comes up.
- If none of the specified LE servers are up or connected to the master LECS and more than one LES is defined for an ELAN, a configuration request for that specific ELAN is rejected by the LECS.
- Changes made to the list of LECS addresses on ATM switches may take up to a minute to propagate through the network. Changes made to the configuration database regarding LES addresses take effect almost immediately.
- If none of the designated LECSs is operational or reachable, the ATM Forum-defined well-known LECS address is used.
- You can override the LECS address on any subinterface, by using the following commands:
    - **lane auto-config-atm-address**
    - **lane fixed-config-atm-address**
    - **lane config-atm-address**

Caution When an override like this is performed, fault-tolerant operation cannot be guaranteed. To avoid affecting the fault-tolerant operation, do not override any LECS, LES or BUS addresses.

- If an underlying ATM network failure occurs, there may be multiple master LECSs and multiple active LE servers for the same ELAN. This situation creates a "partitioned" network. The clients continue to operate normally, but transmission between different partitions of the network is not possible. When the network break is repaired, the system recovers.
- When the LECS is already up and running, and you use the **lane config fixed-config-atm-address**interface commandto configure the well-known LECS address, be aware of the following scenarios:
    - If you configure the LECS with only the well-known address, the LECS will not participate in the SSRP, act as a "standalone" master, and only listen on the well-known LECS address. This scenario is ideal if you want a "standalone" LECS that does not participate in SSRP, and you would like to listen to only the well-known address.
    - If only the well-known address is already assigned, and you assign at least one other address to the LECS, (additional addresses are assigned using the **lane config auto-config-atm-address** interface command and/or the **lane config config-atm-address**interface command) the LECS will participate in the SSRP and act as the master or slave based on the normal SSRP rules. This scenario is ideal if you would like the LECS to participate in SSRP, and you would like to make the master LECS listen on the well-known address.
    - If the LECS is participating in SSRP, has more than one address (one of which is the well-known address), and all the addresses but the well-known address is removed, the LECS will declare itself the master and stop participating in SSRP completely.
    - If the LECS is operating as an SSRP slave, and it has the well-known address configured, it will not listen on the well-known address unless it becomes the master.
    - If you want the LECS to assume the well-known address only when it becomes the master, configure the LECS with the well-known address and at least one other address.

SSRP Changes to Reduce Network Flap

SSRP was originally designed so that when a higher LES came on line, all the LECs in that ELAN flipped over to the higher LES. This caused unnecessary disruptions in large networks. Now SSRP is designed to eliminate unnecessary flapping. If the current LES is healthy, the flapping can be eliminated by changing the SSRP behavior so that the ELAN does not flip over to another LES. Obviously, if the currently active LES goes down, all the LECs will then be switched over to the first available highest LES in the list. This is now the default behavior.

If ELANs are now configured in the new way, an LECS switchover may or may not cause a network flap depending on how quickly each LES now reconnects to the new master LECS. If the old active LES connects first, the flap will not occur. However, if another LES connects first (since now the criteria is that the first connected LES is assumed the master LES, rather than the highest ranking one), then the network will still flap.

For customers who would specifically like to maintain the old SSRP behavior, they can use the new LECS **name** *elan-name* **preempt**LANE database configuration command**.**This command will force the old behavior to be maintained. This feature can be enabled/disabled on a per individual ELAN basis from the LECS database. In the older scheme (preempt), the LES switchover caused network flap.

To enable network flap and set the ELAN preempt for a LES, use the following command in LANE database configuration mode:

Command	Purpose
`Router(lane-config-dat)#` **name** *elan-name* **preempt**	Sets the ELAN LES preemption.

Monitoring and Maintaining the LANE Components

After configuring LANE components on an interface or any of its subinterfaces, on a specified subinterface, or on an ELAN, you can display their status. To show LANE information, use the following commands in EXEC mode:

Command	Purpose
`Router#` **show lane** [**interface atm** *slot*/**0**[.*subinterface-number*] | **name** *elan-name*] [**brief**] `Router#` **show lane** [**interface atm** *slot*/*port-adapter*/**0**[.*subinterface-number*] | **name** *elan-name*] [**brief**] `Router#` **show lane** [**interface atm** *number* [.*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-virtual channel connection LANE information for all the LANE components and emulated LANs configured on an interface or any of its subinterfaces. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
`Router#` **show lane bus** [**interface atm** *slot*/**0**[.*subinterface-number*] | **name** *elan-name*] [**brief**] `Router#` **show lane bus** [**interface atm** *slot*/*port-adapter*/ **0** [.*subinterface-number*] | **name** *elan-name*] [**brief**] `Router#` **show lane bus** [**interface atm** *number* [.*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for the BUS configured on any subinterface or ELAN. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.

Command	Purpose
`Router#` **show lane client** [**interface atm** *slot*/**0**[**.***subinterface-number*] | **name** *elan-name*] [**brief** `Router#` **show lane client** [**interface atm** *slot*/*port-adapter*/**0**[**.***subinterface-number*] | **name** *elan-name*] [**brief**] `Router#` **show lane client** [**interface atm** *number* [**.***subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for all LANE clients configured on any subinterface or ELAN. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
`Router#` **show lane config** [**interface atm** *slot*/**0**] `Router#` **show lane config** [**interface atm** *slot*/*port-adapter*/**0**] `Router#` **show lane config** [**interface atm** *number*]	Displays the global and per-VCC LANE information for the LECS configured on any interface. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
`Router#` **show lane database** [*database-name*]	Displays the LECS's database.
	Displays the automatically assigned ATM address of each LANE component in a router or on a specified interface or subinterface. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.

Command	Purpose
Router# **show lane default-atm-addresses** [**interface atm** *slot*/**0.***subinterface-number*] Router# **show lane default-atm-addresses** [**interface atm** *slot*/*port-adapter*/**0.***subinterface-number*] Router# **show lane default-atm-addresses** [**interface atm** *number***.***subinterface-number*]	
Router# **show lane le-arp** [**interface atm** *slot*/**0** [**.***subinterface-number*] | **name** *elan-name*] Router# **show lane le-arp** [**interface atm** *slot*/*port-adapter*/**0** [**.***subinterface-number*] | **name** *elan-name*] Router# **show lane le-arp** [**interface atm** *number* [**.***subinterface-number*] | **name** *elan-name*]	Display the LANE ARP table of the LANE client configured on the specified subinterface or ELAN. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.
Router# **show lane server** [**interface atm** *slot*/**0** [**.***subinterface-number*] | **name** *elan-name*] [**brief** Router# **show lane server** [**interface atm** *slot*/*port-adapter*/**0** [*.subinterface-number*] | **name** *elan-name*] [**brief**] Router# **show lane server** [**interface atm** *number* [*.subinterface-number*] | **name** *elan-name*] [**brief**]	Display the global and per-VCC LANE information for the LES configured on a specified subinterface or ELAN. • On the AIP for Cisco 7500 series routers; On the ATM port adapter for Cisco 7200 series routers. • On the ATM port adapter for Cisco 7500 series routers. • On the NPM for Cisco 4500 and Cisco 4700 routers.

LANE Configuration Examples

All examples use the automatic ATM address assignment method described in the "Method of Automatically Assigning ATM Addresses, on page 551" section earlier in this chapter. These examples show the LANE configurations, not the process of determining the ATM addresses and entering them.

Single Ethernet ELAN Example

The following example configures four Cisco 7500 series routers for one Ethernet ELAN. Router 1 contains the LECS, the server, the BUS, and a client. The remaining routers each contain a client for the ELAN. This example accepts all default settings that are provided. For example, it does not explicitly set ATM addresses for the different LANE components that are collocated on the router. Membership in this LAN is not restricted.

Router 1 Configuration

```
lane database example1
 name eng server-atm-address 39.000001415555121101020304.0800.200c.1001.01
 default-name eng
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database example1
interface atm 1/0.1
 ip address 172.16.0.1 255.255.255.0
 lane server-bus ethernet eng
 lane client ethernet
```

Router 2 Configuration

```
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 1/0.1
 ip address 172.16.0.3 255.255.255.0
 lane client ethernet
```

Router 3 Configuration

```
interface atm 2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 2/0.1
 ip address 172.16.0.4 255.255.255.0
 lane client ethernet
```

Router 4 Configuration

```
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 1/0.3
 ip address 172.16.0.5 255.255.255.0
 lane client ethernet
```

Single Ethernet ELAN with a Backup LECS and LES Example

This example configures four Cisco 7500 series routers for one ELAN with fault tolerance. Router 1 contains the LECS, the server, the BUS, and a client. Router 2 contains the backup LECS and the backup LES for this ELAN and another client. Routers 3 and 4 contain clients only. This example accepts all default settings that are provided. For example, it does not explicitly set ATM addresses for the various LANE components collocated on the router. Membership in this LAN is not restricted.

Router 1 Configuration

```
lane database example1
 name eng server-atm-address 39.000001415555121101020304.0800.200c.1001.01
 name eng server-atm-address 39.000001415555121101020304.0612.200c 2001.01
 default-name eng
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database example1
interface atm 1/0.1
 ip address 172.16.0.1 255.255.255.0
 lane server-bus ethernet eng
 lane client ethernet
```

Router 2 Configuration

```
lane database example1_backup
 name eng server-atm-address 39.000001415555121101020304.0800.200c.1001.01
 name eng server-atm-address 39.000001415555121101020304.0612.200c 2001.01 (backup LES)
 default-name eng
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database example1_backup
interface atm 1/0.1
 ip address 172.16.0.3 255.255.255.0
 lane server-bus ethernet eng
 lane client ethernet
```

Router 3 Configuration

```
interface atm 2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 2/0.1
 ip address 172.16.0.4 255.255.255.0
 lane client ethernet
```

Router 4 Configuration

```
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 1/0.3
 ip address 172.16.0.5 255.255.255.0
 lane client ethernet
```

Multiple Token Ring ELANs with Unrestricted Membership Example

The following example configures four Cisco 7500 series routers for three emulated LANS for Engineering, Manufacturing, and Marketing, as shown in the figure below. This example does not restrict membership in the emulated LANs.

Figure 37: Multiple Emulated LANs

In this example, Router 1 has the following LANE components:

- The LECS (there is one LECS for this group of emulated LANs)
- The LES and BUS for the ELAN for Manufacturing (*man*)
- The LES and BUS for the ELAN for Engineering (*eng*)
- A LANE client for the ELAN for Manufacturing (*man*)
- A LANE client for the ELAN for Engineering (*eng*)

Router 2 has the following LANE components:

- A LANE client for the ELAN for Manufacturing (*man*)
- A LANE client for the ELAN for Engineering (*eng*)

Router 3 has the following LANE components:

- A LANE client for the ELAN for Manufacturing (*man*)
- A LANE client for the ELAN for Marketing (*mkt*)

Router 4 has the following LANE components:

- The LES and BUS for the ELAN for Marketing (*mkt*)
- A LANE client for the ELAN for Manufacturing (*man*)
- A LANE client for the ELAN for Marketing (*mkt*)

For the purposes of this example, the four routers are assigned ATM address prefixes and end system identifiers (ESIs) as shown in the table below (the ESI part of the ATM address is derived from the first MAC address of the AIP shown in the example).

Table 23: ATM Prefixes for TR-LANE Example

Router	ATM Address Prefix	ESI Base
Router 1	39.000001415555121101020304	0800.200c.1000
Router 2	39.000001415555121101020304	0800.200c.2000
Router 3	39.000001415555121101020304	0800.200c.3000
Router 4	39.000001415555121101020304	0800.200c.4000

Router 1 Configuration

Router 1 has the LECS and its database, the server and BUS for the Manufacturing ELAN, the server and BUS for the Engineering ELAN, a client for Manufacturing, and a client for Engineering. Router 1 is configured as shown in this example:

```
!The following lines name and configure the configuration server's database.
lane database example2
 name eng server-atm-address 39.000001415555121101020304.0800.200c.1001.02
 name eng local-seg-id 1000
 name man server-atm-address 39.000001415555121101020304.0800.200c.1001.01
 name man local-seg-id 2000
 name mkt server-atm-address 39.000001415555121101020304.0800.200c.4001.01
 name mkt local-seg-id 3000
 default-name man
!
! The following lines bring up the configuration server and associate
! it with a database name.
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database example2
!
! The following lines configure the "man" server, broadcast-and-unknown server,
! and the client on atm subinterface 1/0.1. The client is assigned to the default
! emulated lan.
interface atm 1/0.1
 ip address 172.16.0.1 255.255.255.0
 lane server-bus tokenring man
 lane client tokenring man
!
! The following lines configure the "eng" server, broadcast-and-unknown server,
! and the client on atm subinterface 1/0.2. The client is assigned to the
! engineering emulated lan. Each emulated LAN is a different subnetwork, so the "eng"
! client has an IP address on a different subnetwork than the "man" client.
interface atm 1/0.2
 ip address 172.16.1.1 255.255.255.0
 lane server-bus tokenring eng
 lane client tokenring eng
```

Router 2 Configuration

Router 2 is configured for a client of the Manufacturing ELAN and a client of the Engineering ELAN. Because the default ELAN name is *man* , the first client is linked to that ELAN name by default. Router 2 is configured as follows:

```
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 1/0.1
 ip address 172.16.0.2 255.255.255.0
 lane client tokenring
interface atm 1/0.2
 ip address 172.16.1.2 255.255.255.0
 lane client tokenring eng
```

Router 3 Configuration

Router 3 is configured for a client of the Manufacturing ELAN and a client of the Marketing ELAN. Because the default ELAN name is *man* , the first client is linked to that ELAN name by default. Router 3 is configured as shown here:

```
interface atm 2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 2/0.1
 ip address 172.16.0.3 255.255.255.0
 lane client tokenring
interface atm 2/0.2
 ip address 172.16.2.3 255.255.255.0
 lane client tokenring mkt
```

Router 4 Configuration

Router 4 has the server and BUS for the Marketing ELAN, a client for Marketing, and a client for Manufacturing. Because the default ELAN name is *man* , the second client is linked to that ELAN name by default. Router 4 is configured as shown here:

```
interface atm 3/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
interface atm 3/0.1
 ip address 172.16.2.4 255.255.255.0
 lane server-bus tokenring mkt
 lane client tokenring mkt
interface atm 3/0.2
 ip address 172.16.0.4 255.255.255.0
 lane client tokenring
```

Multiple Token Ring ELANs with Restricted Membership Example

The following example, shown in the figure below, configures a Cisco 7500 series router for three emulated LANS for Engineering, Manufacturing, and Marketing.

The same components are assigned to the four routers as in the previous example. The ATM address prefixes and MAC addresses are also the same as in the previous example.

However, this example restricts membership for the Engineering and Marketing emulated LANs. The LECS's database has explicit entries binding the ATM addresses of LANE clients to specified, named emulated LANs. In such cases, the client requests information from the LECS about which ELAN it should join; the LECS checks its database and replies to the client. Since the Manufacturing ELAN is unrestricted, any client not in the LECS's database is allowed to join it.

Figure 38: Multiple Emulated LANs with Restricted Membership

Router 1 Configuration

Router 1 has the LECS and its database, the server and BUS for the Manufacturing ELAN, the server and BUS for the Engineering ELAN, a client for Manufacturing, and a client for Engineering. It also has explicit database entries binding the ATM addresses of LANE clients to specified, named emulated LANs. Router 1 is configured as shown here:

```
! The following lines name and configure the configuration server's database.
lane database example3
 name eng server-atm-address 39.000001415555121101020304.0800.200c.1001.02 restricted
 name eng local-seg-id 1000
 name man server-atm-address 39.000001415555121101020304.0800.200c.1001.01
 name man local-seg-id 2000
 name mkt server-atm-address 39.000001415555121101020304.0800.200c.4001.01 restricted
 name mkt local-seg-id 3000
!
 ! The following lines add database entries binding specified client ATM
 ! addresses to emulated LANs. In each case, the Selector byte corresponds
 ! to the subinterface number on the specified router.
 ! The next command binds the client on Router 1's subinterface 2 to the eng ELAN.
 client-atm-address 39.0000014155551211.0800.200c.1000.02 name eng
 ! The next command binds the client on Router 2's subinterface 2 to the eng ELAN.
 client-atm-address 39.0000014155551211.0800.200c.2000.02 name eng
 ! The next command binds the client on Router 3's subinterface 2 to the mkt ELAN.
 client-atm-address 39.0000014155551211.0800.200c.3000.02 name mkt
 ! The next command binds the client on Router 4's subinterface 1 to the mkt ELAN.
 client-atm-address 39.0000014155551211.0800.200c.4000.01 name mkt
 default-name man
!
! The following lines bring up the configuration server and associate
! it with a database name.
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database example3
!
! The following lines configure the "man" server/broadcast-and-unknown server,
! and the client on atm subinterface 1/0.1. The client is assigned to the default
! emulated lan.
interface atm 1/0.1
 ip address 172.16.0.1 255.255.255.0
 lane server-bus tokenring man
 lane client tokenring
!
! The following lines configure the "eng" server/broadcast-and-unknown server
! and the client on atm subinterface 1/0.2. The configuration server assigns the
! client to the engineering emulated lan.
interface atm 1/0.2
 ip address 172.16.1.1 255.255.255.0
 lane server-bus tokenring eng
 lane client tokenring eng
```

Router 2 Configuration

Router 2 is configured for a client of the Manufacturing ELAN and a client of the Engineering ELAN. Because the default ELAN name is *man* , the first client is linked to that ELAN name by default. Router 2 is configured as shown in this example:

```
interface atm 1/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
! This client is not in the configuration server's database, so it will be
! linked to the "man" ELAN by default.
interface atm 1/0.1
 ip address 172.16.0.2 255.255.255.0
 lane client tokenring
! A client for the following interface is entered in the configuration
! server's database as linked to the "eng" ELAN.
interface atm 1/0.2
```

```
 ip address 172.16.1.2 255.255.255.0
 lane client tokenring eng
```

Router 3 Configuration

Router 3 is configured for a client of the Manufacturing ELAN and a client of the Marketing ELAN. Because the default ELAN name is *man* , the first client is linked to that ELAN name by default. The second client is listed in the database as linked to the *mkt* ELAN. Router 3 is configured as shown in this example:

```
interface atm 2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
! The first client is not entered in the database, so it is linked to the
! "man" ELAN by default.
interface atm 2/0.1
 ip address 172.16.0.3 255.255.255.0
 lane client tokenring man
! The second client is explicitly entered in the configuration server's
! database as linked to the "mkt" ELAN.
interface atm 2/0.2
 ip address 172.16.2.3 255.255.255.0
 lane client tokenring mkt
```

Router 4 Configuration

Router 4 has the server and BUS for the Marketing ELAN, a client for Marketing, and a client for Manufacturing. The first client is listed in the database as linked to the *mkt* emulated LANs. The second client is not listed in the database, but is linked to the *man* ELAN name by default. Router 4 is configured as shown here:

```
interface atm 3/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
! The first client is explicitly entered in the configuration server's
! database as linked to the "mkt" ELAN.
interface atm 3/0.1
 ip address 172.16.2.4 255.255.255.0
 lane server-bus tokenring mkt
 lane client tokenring mkt
! The following client is not entered in the database, so it is linked to the
! "man" ELAN by default.
interface atm 3/0.2
 ip address 172.16.0.4 255.255.255.0
 lane client tokenring
```

TR-LANE with 2-Port SRB Example

The following example configures two Cisco 7500 series routers for one emulated Token-Ring LAN using SRB, as shown in the figure below. This example does not restrict membership in the emulated LANs.

Figure 39: 2-Port SRB TR-LANE

Router 1 Configuration

Router 1 contains the LECS, the server and BUS, and a client. Router 1 is configured as shown in this example:

```
hostname Router1
```

```
!
! The following lines configure the database cisco_eng.
lane database cisco_eng
 name elan1 server-atm-address 39.020304050607080910111213.00000CA05B41.01
 name elan1 local-seg-id 2048
 default-name elan1
!
interface Ethernet0/0
 ip address 10.6.10.4 255.255.255.0
!
! The following lines configure a configuration server using the cisco_eng database on
! the interface. No IP address is needed since we are using source-route bridging.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database cisco_eng
!
! The following lines configure the server-bus and the client on the subinterface and
! specify source-route bridging information.
interface ATM2/0.1 multipoint
 lane server-bus tokenring elan1
 lane client tokenring elan1
 source-bridge 2048 1 1
 source-bridge spanning
!
! The following lines configure source-route bridging on the Token Ring interface.
interface TokenRing3/0/0
 no ip address
 ring-speed 16
 source-bridge 1 1 2048
 source-bridge spanning
!
router igrp 65529
 network 10.0.0.0
```

Router 2 Configuration

Router 2 contains only a client for the ELAN. Router 2 is configured as shown here:

```
hostname Router2
!
interface Ethernet0/0
 ip address 10.6.10.5 255.255.255.0
!
! The following lines configure source-route bridging on the Token Ring interface.
interface TokenRing1/0
 no ip address
 ring-speed 16
 source-bridge 2 2 2048
 source-bridge spanning
!
! The following lines set up the signalling and ILMI PVCs.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
!
! The following lines set up a client on the subinterface and configure
! source-route bridging.
interface ATM2/0.1 multipoint
 ip address 1.1.1.2 255.0.0.0
 lane client tokenring elan1
 source-bridge 2048 2 2
 source-bridge spanning
!
router igrp 65529
 network 10.0.0.0
```

TR-LANE with Multiport SRB Example

The following example configures two Cisco 7500 series routers for one emulated Token-Ring LAN using SRB, as shown in the figure below. Since each router connects to three rings (the two Token Rings and the ELAN "ring"), a virtual ring must be configured on the router. This example does not restrict membership in the emulated LANs.

Figure 40: Multiport SRB Token Ring ELAN

Router 1 Configuration

Router 1 contains the LECS, the server and BUS, and a client. Router 1 is configured as shown in this example:

```
hostname Router1
!
! The following lines configure the database with the information about the
! elan1 emulated Token Ring LAN.
lane database cisco_eng
 name elan1 server-atm-address 39.020304050607080910111213.00000CA05B41.01
 name elan1 local-seg-id 2048
 default-name elan1
!
! The following line configures virtual ring 256 on the router.
source-bridge ring-group 256
!
interface Ethernet0/0
 ip address 10.6.10.4 255.255.255.0
!
! The following lines configure the configuration server to use the cisco_eng database.
! The Signalling and ILMI PVCs are also configured.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database cisco_eng
!
! The following lines configure the server and broadcast-and-unknown server and a client
! on the interface. The lines also specify source-route bridging information.
interface ATM2/0.1 multipoint
 lane server-bus tokenring elan1
 lane client tokenring elan1
 source-bridge 2048 5 256
 source-bridge spanning
!
! The following lines configure the Token Ring interfaces.
interface TokenRing3/0
 no ip address
 ring-speed 16
 source-bridge 1 1 256
 source-bridge spanning
interface TokenRing3/1
 no ip address
 ring-speed 16
 source-bridge 2 2 256
 source-bridge spanning
!
router igrp 65529
 network 10.0.0.0
```

Router 2 Configuration

Router 2 contains only a client for the ELAN. Router 2 is configured as follows:

```
hostname Router2
!
! The following line configures virtual ring 512 on the router.
source-bridge ring-group 512
!
interface Ethernet0/0
 ip address 10.6.10.5 255.255.255.0
!
! The following lines configure the Token Ring interfaces.
interface TokenRing1/0
 no ip address
 ring-speed 16
 source-bridge 3 3 512
 source-bridge spanning
interface TokenRing1/1
 no ip address
 ring-speed 16
 source-bridge 4 4 512
 source-bridge spanning
!
! The following lines configure the signalling and ILMI PVCs.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
!
! The following lines configure the client. Source-route bridging is also configured.
interface ATM2/0.1 multipoint
 ip address 1.1.1.2 255.0.0.0
 lane client tokenring elan1
 source-bridge 2048 6 512
 source-bridge spanning
!
router igrp 65529
 network 10.0.0.0
```

Token Ring and Ethernet Emulated LANs Example

This example, shown in the figure below, configures routing between a Token Ring ELAN (*trelan*) and an Ethernet ELAN (*ethelan*) on the same ATM interface. Router 1 contains the LECS, a LES and BUS for each ELAN, and a client for each ELAN. Router 2 contains a client for *trelan* (Token Ring); Router 3 contains a client for *ethelan* (Ethernet).

Figure 41: Routing Between Token Ring and Ethernet Emulated LANs

Router 1 Configuration

Router 1 contains the LECS, a LES and BUS for each ELAN, and a client for each ELAN. Router 1 is configured as shown in this example:

```
hostname router1
!
! The following lines name and configures the configuration server's database.
! The server addresses for trelan and ethelan and the ELAN ring number for
! trelan are entered into the database. The default ELAN is trelan.
lane database cisco_eng
 name trelan server-atm-address 39.020304050607080910111213.00000CA05B41.01
```

```
 name trelan local-seg-id 2048
 name ethelan server-atm-address 39.020304050607080910111213.00000CA05B41.02
 default-name trelan
!
! The following lines enable the configuration server and associate it
! with the cisco_eng database.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database cisco_eng
!
! The following lines configure the tokenring LES/BUS and LEC for trelan
! on subinterface atm2/0.1 and assign an IP address to the subinterface.
interface ATM2/0.1 multipoint
 ip address 10.1.1.1 255.255.255.0
 lane server-bus tokenring trelan
 lane client tokenring trelan
!
! The following lines configure the Ethernet LES/BUS and LEC for ethelan
! on subinterface atm2/0.2 and assign an IP address to the subinterface.
interface ATM2/0.2 multipoint
 ip address 20.2.2.1 255.255.255.0
 lane server-bus ethernet ethelan
 lane client ethernet ethelan
!
! The following lines configure the IGRP routing protocol to enable routing
! between ELANS.
router igrp 1
 network 10.0.0.0
 network 20.0.0.0
```

Router 2 Configuration

Router 2 contains a client for *trelan* (Token Ring). Router 2 is configured as follows:

```
hostname router2
!
! The following lines set up the signalling and ILMI PVCs for the interface.
interface ATM2/0
 no ip address
 no keepalive
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
!
! The following lines configure a Token Ring LEC on atm2/0.1 and assign
! an IP address to the subinterface.
interface ATM2/0.1 multipoint
 ip address 10.1.1.2 255.255.255.0
 lane client tokenring trelan
!
! The following lines configure the IGRP routing protocol to enable routing
! between ELANS.
router igrp 1
 network 10.0.0.0
 network 20.0.0.0
```

Router 3 Configuration

Router 3 contains a client for *ethelan* (Ethernet). Router 3 is configured as follows:

```
hostname router3
!
! The following lines set up the signalling and ILMI PVCs for the interface.
interface ATM2/0
 no ip address
```

```
 no ip mroute-cache
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
!
! The following lines configure an Ethernet LEC on atm2/0.1 and assign
! an IP address to the subinterface.
interface ATM2/0.1 multipoint
 ip address 20.2.2.2 255.255.255.0
 lane client ethernet ethelan
!
! The following lines configure the IGRP routing protocol to enable routing
! between ELANS.
router igrp 1
 network 10.0.0.0
 network 20.0.0.0
```

Disabling LANE Flush Process Example

The following example shows a running configuration and the LE_FLUSH process disabled for all LECs:

```
more system:running-config
Building configuration...
Current configuration :496 bytes
!
! Last configuration change at 11:36:21 UTC Thu Dec 20 2001
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname donner_b
!
no lane client flush
!
interface ATM0
 atm preferred phy A
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 no atm ilmi-keepalive
!
interface ATM0.1 multipoint
 lane config-atm-address 47.00918100000001007385101.0050A2FEBC43.00
 lane client ethernet 100 elan1
!
line con 0
line vty 0 4
 no login
!
end
```

CHAPTER 23

Configuring Token Ring LAN Emulation

This chapter describes how to configure Token Ring LAN emulation (LANE) on the Catalyst 5000 platform. This feature is supported on the following Catalyst 5000 series ATM modules:

- ATM Dual PHY OC-12 modules (WS-X5161 and WS-X5162)
- ATM Dual OC-3 modules (WS-5167 and WS-X5168)

Support for the Token Ring LANE feature was first introduced in Cisco IOS Release 12.0(7)T.

Note Beginning with Cisco IOS Release 11.3, all commands supported on the Cisco 7500 series routers are also supported on the Cisco 7000 series.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Token Ring LANE on ATM

LANE bridges LAN traffic across an ATM network. The Catalyst 5000 Series Token Ring LANE feature emulates an IEEE 802.5 Token Ring LAN using ATM technology. LANE is transparent to upperlayer protocols and applications. No changes are required to existing upperlayer protocols and applications. With Token Ring LANE, Token Ring packets are encapsulated in the appropriate ATM cells and sent across the ATM network. When the packets reach the other side of the ATM network, they are deencapsulated.

Benefits

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (constant transmission delay and guaranteed capacity) with those of packet switching (flexibility and efficiency for intermittent traffic). Like X.25 and Frame Relay, ATM defines the interface between the user equipment (such as workstations and routers) and the network (referred to as the User-Network Interface [UNI]).

Token Ring LANE allows Token Ring LAN users to take advantage of the benefits of ATM without modifying end-station hardware or software. ATM uses connection-oriented service with point-to-point signalling or multicast signalling between source and destination devices. However, Token Ring LANs use connectionless service. Messages are broadcast to all devices on the network. With Token Ring LANE, routers and switches emulate the connectionless service of a Token Ring LAN for the end stations.

By using Token Ring LANE, you can scale your networks to larger sizes while preserving your investment in LAN technology.

Note The Catalyst 5000 series Cisco IOS Token Ring LANE software does not support Ethernet LANE or RFC 1483 permanent virtual connections (PVCs).

LANE Token Ring Components

LANE defines emulated LANs (ELANs). An ELAN consists of the following components:

- LANE client (LEC)--A LEC emulates a LAN interface to higher-layer protocols and applications. It forwards data to other LANE components and performs LANE address resolution functions. Each LEC is a member of only one ELAN. However, a switch or a Catalyst ATM module can include LECs for multiple ELANs; there is one LEC for each ELAN of which it is a member.

If a switch has LECs for multiple ELANs, the switch can route traffic between ELANs.

- LANE server (LES)--The LES is the control center for an ELAN. It provides joining, address resolution, and address registration services to the LECs in that ELAN. LECs can register destination unicast and multicast MAC address with the LES. The LES also handles LANE Address Resolution Protocol (LE_ARP) requests and responses and maintains a list of route descriptors that is used to support source-route bridging (SRB) over ELANs. The route descriptors are used to determine the ATM address of the next hop in the frame’s routing information field (RIF).

There is one LES per ELAN.

- LANE broadcast and unknown server (BUS)--The BUS floods unknown destination traffic and forwards multicast and broadcast traffic to LECs within an ELAN.

One combined LES and BUS is required for each ELAN.

- LANE Configuration Server (LECS)--The LECS contains the database that determines which ELAN a device belongs to (each LECS can have a different database). Each LEC contacts the LECS once to determine which ELAN it should join. The LECS returns the ATM address of the LES for that ELAN.

One LECS is required for each ATM LANE switch cloud.

The LECS database can have the following types of entries:

-
    - ELAN name, ATM address of LES pairs
    - ELAN name and the ring number of the ELAN (local-seg-id)
    - LEC MAC address, ELAN name pairs
    - LEC ATM template, ELAN name pairs
    - Default ELAN name

Note An ELAN name must be unique on an interface. If two interfaces participate in LANE, the second interface may be in a different switch cloud.

The server assigns individual LECs to particular ELANs by directing them to the LES for the ELAN. The LECS maintains a database of LEC and server ATM or MAC addresses and their ELANs. A LECS can serve multiple ELANs.

- Fast Simple Server Redundancy Protocol (FSSRP)--Token Ring LANE relies on three servers: LECS, LES, and BUS. If any one of these servers fails, the ELAN cannot fully function.

Cisco has developed a fault tolerant mechanism known as Simple Server Redundancy Protocol (SSRP) that eliminates these single points of failure. Although there is only one LES per ELAN, SSRP allows you to configure redundant servers. You can configure servers to act as backup servers that become active if a master server fails. The priority levels for the servers determine which servers have precedence.

FSSRP is an enhancement to the SSRP. With FSSRP, LECs no longer need to go down whenever there is a change in the master LES. This uninterrupted service is achieved by connecting the LECs simultaneously to more than one LES/BUS (up to four) so that if the master LES goes down, the backup LESs are immediately available. With the basic SSRP, the LEC must go down and completely recycle before coming back up. This operation is accomplished by keeping the control connections open to all of the active LESs and BUSs in the ELAN. Although this method uses more virtual circuits (VCs), the main benefits are the transparency and speed in the switchover.

Note ELAN components coexist on one or more Cisco routers or Catalyst switches that contain an ATM module. On Cisco routers or Catalyst switches the LES and the BUS are combined into a single entity.

Network Support

In this release, Cisco supports the following networking features:

- Ethernet-emulated LANs
    - Routing from one ELAN to another via IP, IPX, or AppleTalk
    - Bridging between emulated LANs and between emulated LANs and other LANs
    - DECnet, Banyan VINES, and XNS routed protocols
- Token-Ring emulated LANs
    - IP routing (fast switched) between emulated LANs and between a Token Ring ELAN and a legacy LAN
    - IPX routing between emulated LANs and between a Token Ring ELAN and a legacy LAN
    - Two-port and multiport SRB (fast switched) between emulated LANs and between emulated LANs and a Token Ring
    - IP and IPX multiring
    - SRB, source-route translational bridging (SR/TLB), and source-route transparent bridging (SRT)
    - AppleTalk for (IOS) TR-LANE and includes Appletalk fast switched routing.
    - DECnet, Banyan VINES, and XNS protocols are not supported

Cisco’s implementation of LAN Emulation over 802.5 uses existing terminology and configuration options for Token Rings, including SRB. For more information about configuring SRB, see the chapter "Configuring Source-Route Bridging" in the Cisco IOS Bridging and IBM Networking Configuration Guide. Transparent bridging and Advanced Peer-to-Peer Networking (APPN) are not supported at this time.

- Hot Standby Router Protocol (HSRP)

For information about configuring APPN over Ethernet LANE, refer to the "Configuring APPN" chapter in the Cisco IOS Bridging and IBM Networking Configuration Guide.

Restrictions

Before you implement Token Ring LANE, be aware of the following restrictions:

Caution While VLAN Trunking Protocol (VTP) Version 2 must be enabled on a Catalyst 5000 for Token Ring to function, do not use VTP to distribute VLAN configuration information between the switches. Configure the switches to operate in VTP transparent mode and manually configure the VLANs on each switch.

- If you plan to run both Ethernet and Token Ring LANE, the Ethernet LANE software and the Token Ring LANE software must be run on separate ATM modules.
- All ATM switches have identical lists of the global LECS addresses with the identical priorities.

- Ensure that the spanning-tree port cost and priority for the ATM port are configured so that the ATM port is the preferred path (the lowest port cost with the highest priority).
- Only one LEC can be defined for each subinterface. Up to 256 subinterfaces per ATM module can be configured.
- Do not create more than one LEC for each Token Ring Bridge Relay Function (TrBRF) in each ATM module.

While you can have only one LEC for each TrBRF in each module, you can have more than one module installed. These additional modules allow you to have more than one LEC per TrBRF, which means the module can participate in more than one ELAN. The ELANs, however, cannot be parallel or the Spanning-Tree Protocol will block one of the connections.

Note Configuring more than one LEC for a TrBRF on a single ATM module will adversely affect frame forwarding.

- Do not configure parallel ELANs within a TrBRF (parallel ELANs are those ELANs that form a loop between switches).
- Do not create more than one LEC for each Token Ring Concentrator Relay Function (TrCRF) per ATM module.
- Ensure that all-routes explorer (ARE) reduction is enabled (using the set tokenring reduction enable command) on the Token Ring module.
- The number of LESs that can be defined per ELAN is unlimited; however, only one LES per ELAN can be active at a time.
- When a LECS switchover occurs, no previously joined clients are affected.
- In a LES/BUS switchover, there is a momentary loss of clients until all clients are transferred to the new LES/BUS.
- LECSs automatically come up as masters until a higher-level LECS takes priority.
- Using FSSRP, you can configure redundant LESs or BUSs and LECSs to reduce the possibility of a server failure resulting in loss of communication on the LANE network. With redundant LES/BUSs and LECSs, LANE components can switch automatically to the backup LES/BUS or LECS if the primary server fails. For specific information on how to configure FSSRP, refer to the Configuring Fast SSRP for Redundant LANE Services, on page 614 section.

Note FSSRP works only with LECS and LES/BUS combinations on Cisco devices. Third-party LANE components interoperate with the LECS and LES/BUS functions of Cisco devices but cannot take advantage of the redundancy features. Additionally, FSSRP-unaware LECs on Cisco equipment cannot take advantage of FSSRP LES/BUS redundancy.

- When a higher-priority LES comes online, it bumps the current LES off the same ELAN. For a short time after power on, some clients might change from one LES to another, depending upon the order of the LESs coming up.

- If no LES/BUS pair is up or connected to the master LECS, and more than one LES/BUS is defined for an ELAN, the LECS rejects any configuration request for that specific ELAN.
- Changes made to the list of LECS addresses on ATM switches can take up to 1 minute to propagate through the network. Changes made to the LECS database regarding LES addresses take effect almost immediately.
- If no LECS is operational or reachable, the "well-known" LECS address defined by the ATM Forum is used.
- The LECS to be used can be overridden on any subinterface by entering the following commanf:

```
lane config-atm address
 atm-address template
```

Note To avoid affecting the LES/BUS or LEC redundancy, do not override any LECS, LES, or BUS addresses.

- In an underlying ATM network failure, there can be multiple master LECS and multiple active LESs or BUSs for the same ELAN, resulting in a partitioned network. Clients continue to operate normally, but transmission between partitions of the network is not possible. The system recovers when the network break is repaired.

Prerequisites

Token Ring LANE requires that the Catalyst 5000 series switch contain one of the following ATM modules running ATM software Release 4.9b or later:

- ATM Dual PHY OC-12 (WS-X5161 and WS-X5162)
- ATM Dual PHY OC-3 (WS-X5167 and WS-X5168)

These ATM modules provide an ATM network interface for the Catalyst 5000 series switch. Network interfaces reside on modular interface processors, which provide a direct connection between the high-speed synergy backplane and the external networks. The maximum number of ATM modules that the switch supports depends on the bandwidth configured.

The Catalyst 5000 series Token Ring LANE software also requires the Catalyst 5000 series supervisor engine software Release 4.3(1a) or later and one of the following switches:

- Cisco LightStream 1010 with Cisco IOS Release 12.0(1)W5 or later (recommended)
- Any ATM switch with UNI 3.0/3.1 and Interim Local Management Interface (ILMI) support for communicating the LECS address

Note If you plan to run both Ethernet and Token Ring LANE, the Ethernet LANE software and the Token Ring LANE software must be run on separate ATM modules.

Token Ring LANE Configuration Task List

Note There can be multiple LECSs in an ATM cloud.

Before configuring Token Ring LANE, you must first open a session with the ATM module in the Catalyst 5000 series switch by entering the session line configuration command from the supervisor Console> prompt. After opening the session, you see the ATM> prompt. You only have direct access to the ATM module with which you have established a session.

Note The ATM module uses a subset of the Cisco IOS software. Generally, the Cisco IOS software works the same on the ATM module as it does on routers. After configuring the ATM module, you are ready to implement LANE.

Opening a Session from the Switch to the ATM Module

Use the **session** *mod_num* line configuration command to open a session to the ATM module from the Catalyst 5000 family switch in which the module is installed.

This example shows how to create a session to an ATM module installed in slot 5 of the Catalyst 5000 switch:

```
Console> (enable) session 5
Trying ATM-5...
Connected to ATM-5.
Escape character is '^]'.

ATM>
```

After opening the session, you see the ATM> prompt. You then have direct access only to the ATM module with which you have established a session.

Note The ATM module uses a subset of Cisco IOS software. Generally, Cisco IOS software works the same on the ATM module as it does on routers.

To configure the ATM module, you must use the ATM configuration mode in the Cisco IOS software. To enter global configuration mode, enter the configure EXEC command at the privileged EXEC prompt (ATM#). You see the following message, which asks you to specify the terminal, the NVRAM, or a file stored on a network server as the source of configuration commands:

```
Configuring from terminal, memory, or network [terminal]?
```

If you specify terminal, the run-time configuration is used. You can then save the run-time configuration into the NVRAM. If you specify memory, the run-time configuration is updated from the NVRAM. If you specify network, the run-time configuration is updated from a file in a server on the network.

Note You cannot configure from the network.

The ATM module accepts one configuration command per line. You can enter as many configuration commands as you want.

You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!) or pound sign (#). Comments are not stored in NVRAM or in the active copy of the configuration file. In other words, comments do not appear when you list the active configuration with the write terminal EXEC command or list the configuration in NVRAM with the show configuration EXEC command. Comments are stripped out of the configuration file when it is loaded to the ATM module.

Creating a LANE Plan and Worksheet

Before you begin to configure Token Ring LANE, you must decide whether you want to set up one or multiple ELANs. If you set up multiple ELANs, you must also decide where the servers and LECs will be located, and whether to restrict the clients that can belong to each ELAN. Bridged ELANs are configured just like any other LAN, in terms of commands and outputs. Once you have made those decisions, you can configure Token Ring LANE.

Before implementing Token Ring LANE, it might help you to begin by drawing up a plan and a worksheet for your own LANE scenario, showing the following information and leaving space to note the ATM address of each LANE component on each subinterface for each participating switch:

- Catalyst 5000 series switch interface where the LECS will be located.
- Catalyst 5000 series switch interface and subinterface where the LES/BUS for each ELAN will be located. For fault-tolerant operation, multiple servers can be on each ELAN.
- Catalyst 5000 series switch ATM modules, subinterfaces, and VLANs where the LECs for each ELAN will be located.
- Name of the default ELAN (optional). The default Token Ring ELAN is the same as the default TrCRF (1003). You can use the default Token Ring ELAN (trcrf-default) or configure a new one.
- Names of the ELANs that will have unrestricted membership.
- Names of the ELANs that will have restricted membership.
- Local segment ID for the ELAN. The local segment ID must be identical to the ring number of the TrCRF.

Note The last three items in the list above are important because they determine how you set up each ELAN in the LECS database.

Default LANE Configuration

The table below shows the default LANE configuration.

Table 24: Default LANE Configuration

Feature	Default Value
LANE components	No LECS database is configured. No LES/BUS is configured. No LECs are configured.
PVCs	ILMI and signalling PVCs are set up.
Preferred PHY (Dual PHY modules only)	PHY A
Output throttling	Disabled
ILMI keepalives	Disabled
UNI version	Autonegotiate (reverts to UNI 3.0 if autonegotiation fails)
VTP	Disabled

Configuring the ATM Module from the Terminal

To configure the ATM module from the terminal, use the following commands beginning in privileged EXEC mode:

SUMMARY STEPS

1. ATM# **configure terminal**
2. ATM(config)# **interface atm**>*elanname*
3. ATM(config-if)# **lane client tokenring**>*elanname*
4. ATM(config-if)# **Ctrl-Z**
5. ATM(config)# **write memory**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM# **configure terminal**	Selects the terminal option and enters global configuration mode.
Step 2	ATM(config)# **interface atm**>*elanname*	Selects an ATM ELAN subinterface.
Step 3	ATM(config-if)# **lane client tokenring**>*elanname*	Identifies the ELAN attached to this subinterface as a Token Ring ELAN.

	Command or Action	Purpose
Step 4	ATM(config-if)# **Ctrl-Z**	Exits global configuration mode.
Step 5	ATM(config)# **write memory**	Saves the configuration file modifications to NVRAM.

What to Do Next

In the following example, the ATM module is configured from the terminal. The interface atm 0 interface configuration command designates that ATM interface 0 is to be configured. The lane client tokenring command links TrCRF 10 to the ELAN named trcrf-10. The Ctrl-Z command quits configuration mode. The write memory command loads the configuration changes into NVRAM on the ATM module.

```
ATM# configure terminal
ATM (config)# interface atm 0
ATM (config-subif)# lane client tokenring 10 trcrf-10
ATM (config-subif)# Ctrl-Z
ATM# write memory
```

NVRAM stores the current configuration information in text format as configuration commands, recording only nondefault settings. The ATM module software performs a memory checksum to guard against corrupted data.

As part of its startup sequence, the ATM module startup software always checks for configuration information in NVRAM. If NVRAM holds valid configuration commands, the ATM module executes the commands automatically at startup. If the ATM module detects a problem with its NVRAM or the configuration it contains, the module goes into default configuration. Problems can include a bad checksum for the information in NVRAM or the absence of critical configuration information.

Configuring the ATM Module from NVRAM

To configure the ATM module from NVRAM, reexecute the configuration commands in privileged EXEC mode:

Command	Purpose
ATM(config)# **configure memory**	Configures the ATM module from NVRAM.

Configuring the Prefix on the LightStream 1010 Switch

Before you configure LANE components on a Catalyst 5000 series switch ATM module, you must configure the Cisco LightStream 1010 switch with the ATM address prefix to be used by all LANE components in the switch cloud.

> **Note** On the Cisco LightStream 1010 switch, the ATM address prefix is called the *node ID*. Prefixes must be 26 digits long. If you provide fewer than 26 digits, zeros are added to the right of the specified value to fill it to 26 digits. LANE prefixes must start with 39 or 47.

> **Note** If you do not save the configured value permanently, it will be lost when the switch is reset or powered off.

To display the current prefix on the Cisco LightStream 1010 switch, use the **show network** EXEC command.

To set the ATM address prefix, use the following commands on the Cisco LightStream 1010 switch beginning in global configuration mode:

SUMMARY STEPS

1. Switch(config)# **atm address** {*atm_address* | *prefix...* }
2. Switch(config)# **exit**
3. Switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Switch(config)# **atm address** {*atm_address* | *prefix...* }	Sets the local node ID (prefix of the ATM address).
Step 2	Switch(config)# **exit**	Exits global configuration mode.
Step 3	Switch# **copy running-config startup-config**	Saves the configuration values permanently.

Setting Up the Signalling PVC

You must set up the signalling PVC and the PVC that will communicate with the ILMI on the major ATM interface of any Catalyst 5000 series switch that participates in LANE. Complete this task only once for a major interface. You need not repeat this task on the same interface even though you might configure LESs and clients on several of its subinterfaces.

To set up these PVCs, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. ATM(config)# **interface atm***slot*/*port*
2. ATM(config)# **atm pvc***vcd vpi vci* **qsaal**
3. ATM(config)# **atm pvc***vcd vpi vci***ilmi**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM(config)# **interface atm***slot*/*port*	Specifies the major ATM interface and enters interface configuration mode.
Step 2	ATM(config)# **atm pvc***vcd vpi vci* **qsaal**	Establishes the signalling PVC that sets up and tears down switched virtual circuits (SVCs); the *vpi* and *vci* values are usually set to 0 and 5, respectively. The *vcd* is the virtual channel descriptor.
Step 3	ATM(config)# **atm pvc***vcd vpi vci***ilmi**	Sets up a PVC to communicate with the ILMI; the *vpi* and *vci* values are usually set to 0 and 16, respectively.

Displaying LANE Default Addresses

You can display the LANE default addresses to make configuration easier. Complete this task for each router that participates in LANE. This command displays default addresses for all ATM interfaces present on the router. Write down the displayed addresses on your worksheet.

To display the default LANE addresses, use the following command in EXEC mode:

Command	Purpose
`Router#` **show lane default-atm-addresses**	Displays the LANE default addresses.

Entering the LECS ATM Address on the LightStream 1010 Switch

You must enter the LECS ATM address into each ATM switch (such as a Cisco LightStream 1010 ATM switch) connected to an ATM module in your LANE network and save the address permanently so that the value will not be lost when the switch is reset or powered off. Programming the LECS addresses allows the LESs and LECs to determine the LECS addresses dynamically through ILMI.

To enter a LECS ATM address into a LightStream 1010 switch and save it there permanently, use the following commands on the Cisco LightStream 1010 switch beginning in global configuration mode:

SUMMARY STEPS

1. Switch(config)# **atm lecs-address-default address1** [*address2...*]
2. Router(config)# **exit**
3. Switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Switch(config)# **atm lecs-address-default address1** [*address2...*]	Specifies the LECS's ATM address for the entire switch. Use the addresses from your LANE worksheet and specify the full 40-digit ATM address.
Step 2	Router(config)# **exit**	Exits global configuration mode.
Step 3	Switch# **copy running-config startup-config**	Saves the configuration value permanently.

Configuring the LECS Database

The LECS database contains LANE configuration information, including ELAN name-to-LES/BUS ATM address mappings, LEC address-to-ELAN name mappings, and the name of the default ELAN, if specified. You must configure at least one LECS database in the LANE network.

When configuring the LECS database, remember the following guidelines:

- You can configure redundant LECSs. Redundant LECSs should be configured on different devices in the LANE network. If you configure more than one LECS, make sure that all databases with the same name are identical.
- You can specify one default ELAN in the database. The LECS assigns any client that does not request a specific ELAN to the default ELAN.
- ELANs are either restricted or unrestricted. The LECS assigns a client to an unrestricted ELAN if the client specifies that particular ELAN in its configuration. However, the LECS only assigns a client to a restricted ELAN if the client is specified in the LECS's database as belonging to that ELAN. The default ELAN should have unrestricted membership.
- If you are configuring fault tolerance, you can have any number of servers per ELAN. Priority is determined by entry order; the first entry has the highest priority unless you override it with the index option.

When setting up the LECS database remember that the following are requirements when configuring LECs:

- The VLAN name must match the ELAN name.
- The ring number defined when configuring the VLAN must match the local segment ID.

The **set vlan** interface configuration command assumes that any ring number you enter is in hexadecimal. Therefore, 12 is stored as the hexadecimal value 0x12. The **name** *elan_name* **local-seg-id** *segment_number*LANE database configuration command assumes that any value you enter for the **local-seg-id** is in decimal unless you enter it explicitly in hexadecimal. For example, to define a TrCRF with a ring number of 12 you could enter the **set vlan 12 name crf12 type trcrf ring 12 parent 100** interface configuration command or the **set vlan 12 name crf12 type trcrf ring 0x12 parent 100** interface configuration command.

When defining a corresponding LEC, you could enter the name **crf12 local-seg-id 0x12** or **name crf12 local-seg-id 18** LANE database configuration command because 18 is the decimal equivalent of 0x12.

To set up the database, complete the tasks in the following sections as appropriate for your ELAN plan and scenario:

Setting Up the Database for the Default ELAN

When you configure a Catalyst 5000 series switch ATM module as the LECS for one default ELAN, you need to provide the following information:

- A name for the database
- The ATM address of the LES for the ELAN
- A default name for the ELAN

In addition, you indicate that the LECS's ATM address is to be computed automatically.

The default ELAN cannot be a restricted-membership ELAN. You do not need to specify the ATM or MAC addresses of the LECs for the default ELAN.

On the Dual PHY ATM modules, you must configure redundant LESs or BUSs and a LECS, one for each PHY.

When you configure a database with only a default unrestricted ELAN, you need not specify where the LECs are located. That is, when you set up the LECS's database for a single default ELAN, you need not provide any database entries that link the ATM addresses of any clients with the ELAN name. All of the clients are automatically assigned to a default ELAN.

Note After you configure the LECS database, you must bind the LECS database to the major ATM interface (ATM0) on the ATM module. For information on how to bind the database to the interface, see the Binding the LECS to the ATM Interface, on page 607 section later on in this chapter.

To set up the LECS for a default ELAN, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. ATM(config)# **lane database***database-name*
2. ATM(lane-config-database)# **name***elan -name***server-atm-address***atm-address* [**index** *n*]
3. ATM(lane-config-database)# **name***elan -name***local-seg-id***segment-number*
4. ATM(lane-config-database)# **default-name***elan -name*
5. ATM(lane-config-database)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM(config)# **lane database***database-name*	Enters database configuration mode for the LANE database that you specify.
Step 2	ATM(lane-config-database)# **name***elan -name***server-atm-address***atm-address* [**index** *n*]	Binds the name of the ELAN to the ATM address of the LES in the configuration database. The index determines the priority. The highest priority is 0.

	Command or Action	Purpose
		Enter the ATM address of the server for the specified ELAN, as noted in your LANE worksheet and obtained in the Displaying LANE Default Addresses, on page 556 section. You can have any number of servers per ELAN for fault tolerance. Priority is determined by entry order. The first entry has the highest priority unless you override it with the index number.
Step 3	ATM(lane-config-database)# **name***elan -name***local-seg-id***segment-number*	Assigns a segment number to the emulated Token Ring LAN in the configuration database. The segment number you specify for the **local-seg-id** keyword must remain the same for each entry you add and it must also be identical to the ring number of the TrCRF. The **set vlan**interface configuration command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal.
Step 4	ATM(lane-config-database)# **default-name***elan -name*	Provides a default name for the ELAN in the configuration database. If you are setting up only a default ELAN, the *elan-name* argument in Step 2 and Step 3 is the same as the default ELAN name you provide in Step 4.
Step 5	ATM(lane-config-database)# **exit**	Exits from database configuration mode and returns to global configuration mode.

Setting Up the Database for Unrestricted-Membership ELANs

When you configure unrestricted-membership ELANs in the LECS database, you create database entries that link the name of each ELAN to the ATM address of its LES/BUS.

However, you may choose not to specify where the LECs are located. That is, when you set up the LECS's database, you do not have to provide any database entries that link the ATM addresses or MAC addresses of any clients with the ELAN name. The LECS assigns the clients to the ELANs specified in the client's configurations.

Note In the steps listed in the task table, enter the ATM address of the server for the specified ELAN, as noted in your LANE worksheet and obtained in the Displaying LANE Default Addresses, on page 556 section earlier in this chapter.

To configure unrestricted-membership ELANs in the LECS database, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. ATM(config)# **lane database***database-name*
2. ATM(lane-config-database)# **name***elan-name1***server-atm-address***atm-address* [**index** *n*]
3. ATM(lane-config-database)# **name***elan-name2***server-atm-address***atm-address* [**index** *n*]
4. ATM(lane-config-database)# **name***elan -name1***local-seg-id***segment-number*
5. ATM(lane-config-database)# **name***elan -name2***local-seg-id***segment-number*
6. ATM(lane-config-database)# **default-name***elan-name*
7. ATM(lane-config-database)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM(config)# **lane database***database-name*	Enters database configuration mode for the LANE database that you specify.
Step 2	ATM(lane-config-database)# **name***elan-name1***server-atm-address***atm-address* [**index** *n*]	Binds the name of the first ELAN to the ATM address of the LES/BUS for that ELAN in the configuration database. The index determines the priority. The highest priority is 0.
Step 3	ATM(lane-config-database)# **name***elan-name2***server-atm-address***atm-address* [**index** *n*]	Binds the name of the second ELAN to the ATM address of the LES/BUS in the configuration database. The index determines the priority. The highest priority is 0. Repeat this step, providing a different ELAN name and ATM address for each additional ELAN in this switch cloud.
Step 4	ATM(lane-config-database)# **name***elan -name1***local-seg-id***segment-number*	Assigns a segment number to the first emulated Token Ring LAN in the configuration database. The segment number you specify for **local-seg-id** must be identical to the ring number of the TrCRF. The **set vlan**command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* command assumes that any value you enter for the **local-seg-id** is in decimal unless you enter it explicitly in hexadecimal.
Step 5	ATM(lane-config-database)# **name***elan -name2***local-seg-id***segment-number*	Assigns a segment number to the second emulated Token Ring LAN in the configuration database. The segment number you specify for **local-seg-id** must be identical to the ring number of the TrCRF. The **set vlan**command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* command assumes that any value you enter for the **local-seg-id** is in decimal unless you enter it explicitly in hexadecimal. Repeat this step, providing a different ELAN name and segment number for each additional source-route bridged ELAN in this switch cloud.

	Command or Action	Purpose
Step 6	ATM(lane-config-database)# **default-name***elan-name*	(Optional) Specifies a default ELAN for LECs not explicitly bound to an ELAN.
Step 7	ATM(lane-config-database)# **exit**	Exits database configuration mode and returns to global configuration mode.

Setting Up the Database for Restricted-Membership ELANs

When you configure restricted-membership ELANs in the LECS database, you create database entries that link the name of each ELAN to the ATM address of its LES/BUS.

Unlike unrestricted-membership, you must also specify where the LECs are located. That is, for each restricted-membership ELAN, you provide a database entry that explicitly links the ATM address or MAC address of each client of that ELAN with the name of that ELAN.

Those client database entries specify which clients are allowed to join the ELAN. When a client requests to join an ELAN, the LECS consults its database and then assigns the client to the ELAN specified in the LECS's database.

When clients for the same restricted-membership ELAN are located in multiple switch ATM interfaces, each client's ATM address or MAC address must be linked explicitly with the name of the ELAN. As a result, you must configure as many client entries as you have clients for ELANs in all the switch ATM interfaces. Each client will have a different ATM address in the database entries.

To configure restricted-membership ELANs in the LECS database, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. ATM(config)# **lane database***database-name*
2. ATM(lane-config-database)# **name***elan-name1***server-atm-address***atm-address* **restricted** [**index** *n*]
3. ATM(lane-config-database)# **name***elan-name2***server-atm-address***atm-address* **restricted** [**index** *n*]
4. ATM(lane-config-database)# **name***elan -name1***local-seg-id***segment-number*
5. ATM(lane-config-database)# **name***elan -name2***local-seg-id***segment-number*
6. ATM(lane-config-database)# **client-atm-address***atm-address-template***name***elan-name*
7. ATM(lane-config-database)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM(config)# **lane database***database-name*	Enters database configuration mode for the LANE database that you specify.

	Command or Action	Purpose
Step 2	ATM(lane-config-database)# **name***elan-name1***server-atm-address***atm-address* **restricted** [**index** *n*]	Binds the name of the first ELAN to the ATM address of the LES/BUS for that ELAN in the configuration database. If you are configuring SSRP, repeat this step with the same ELAN name but with different server ATM addresses for each additional server for the same ELAN. The index determines the priority. The highest priority is 0.
Step 3	ATM(lane-config-database)# **name***elan-name2***server-atm-address***atm-address* **restricted** [**index** *n*]	Binds the name of the second ELAN to the ATM address of the LES/BUS in the configuration database. The index determines the priority. The highest priority is 0. Repeat this step, providing a different name and a different ATM address, for each additional ELAN.
Step 4	ATM(lane-config-database)# **name***elan -name1***local-seg-id***segment-number*	Assigns a segment number to the first emulated Token Ring LAN in the configuration database. The segment number you specify for the **local-seg-id** keyword must be identical to the ring number of the TrCRF. The **set vlan**interface configuration command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal.
Step 5	ATM(lane-config-database)# **name***elan -name2***local-seg-id***segment-number*	Assigns a segment number to the second emulated Token Ring LAN in the configuration database. The segment number you specify for the **local-seg-id** keyword must be identical to the ring number of the TrCRF. The **set vlan**interface configuration command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal. Repeat this step, providing a different ELAN name and segment number for each additional source-route bridged ELAN in this switch cloud.
Step 6	ATM(lane-config-database)# **client-atm-address***atm-address-template***name***elan-name*	Adds a database entry associating a specific client's ATM address with a specific restricted-membership ELAN. Repeat this step for each of the clients of each of the restricted-membership ELANs on the switch cloud, in each case specifying that client's ATM address and the name of the ELAN with which it is linked.

	Command or Action	Purpose
Step 7	ATM(lane-config-database)# **exit**	Exits from database configuration mode and returns to global configuration mode.

Binding the LECS to the ATM Interface

Once you have created the database entries as appropriate to the type and the membership conditions of the ELANs, to enable the LECS on the selected ATM interface and switch, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. ATM(config)# **interface atm***number*
2. ATM(config-if)# **lane config auto-config-atm-address**
3. ATM(config-if)# **lane config database***database-name*
4. ATM(config-if)# **exit**
5. ATM# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM(config)# **interface atm***number*	If you are not currently configuring the interface, specifies the major ATM interface where the LECS is located and enters interface configuration mode.
Step 2	ATM(config-if)# **lane config auto-config-atm-address**	Specifies that the LECS's ATM address will be computed by the automatic method.
Step 3	ATM(config-if)# **lane config database***database-name*	Binds the LECS's database name to the specified major interface, and enables the LECS.
Step 4	ATM(config-if)# **exit**	Exits interface configuration mode.
Step 5	ATM# **copy running-config startup-config**	Saves the configuration.

Setting Up a LES BUS and a LEC

For each Catalyst 5000 series switch ATM module that will participate in LANE, set up the necessary servers and clients for each ELAN and then display and record the server and client ATM addresses. Be sure to keep track of the switch ATM interface where the LECS will eventually be located.

If you will have only one default ELAN, you only need to set up one server. If you will have multiple ELANs, you can set up the server for another ELAN on a different subinterface on the same interface of this switch, or you can place it on a different switch.

When you set up a server and BUS on a switch, you can combine them with a client on the same subinterface, a client on a different subinterface, or no client at all on the switch.

Depending on where your clients and servers are located, perform one of the following tasks for each LANE subinterface:

Setting Up the LES BUS for an ELAN

To set up the LES/BUS for an ELAN, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. ATM(config)# **interface atm***number* [**.***subinterface-number*]
2. ATM(config-if)# **lane server-bus tokenring***elan-name1*
3. Repeat Steps 1 and 2 for all LES/BUSs you want to configure on the ATM module.
4. ATM(config-if)# **exit**
5. ATM# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM(config)# **interface atm***number* [**.***subinterface-number*]	Specifies the subinterface for the first ELAN on this switch and enters interface configuration mode.
Step 2	ATM(config-if)# **lane server-bus tokenring***elan-name1*	Enables a LES/BUS for the first ELAN on the subinterface (you cannot configure more than one LES/BUS per subinterface).
Step 3	Repeat Steps 1 and 2 for all LES/BUSs you want to configure on the ATM module.	
Step 4	ATM(config-if)# **exit**	Exits interface configuration mode.
Step 5	ATM# **copy running-config startup-config**	Saves the configuration.

What to Do Next

If the ELAN specified in Step 2 is intended to have restricted membership in the LECS database , carefully consider whether or not you want to specify its name here. You will specify the name in the LECS database when it is set up. However, if you link the client to an ELAN in this step, and through some mistake it does not match the database entry linking the client to an ELAN, this client will not be allowed to join this ELAN or any other.

If you do decide to include the name of the ELAN linked to the client in Step 2 and later want to associate that client with a different ELAN, make the change in the LECS's database before you make the change for the client on this subinterface.

Setting Up a LEC for an ELAN

This section describes the following tasks for setting up a LEC:

- Guidelines for Setting Up a LEC, on page 609
- Creating a Token Ring VLAN, on page 611
- Setting Up the Token Ring VLAN on a LEC, on page 612

Guidelines for Setting Up a LEC

The Catalyst 5000 series Token Ring LANE requires the following software:

- Catalyst 5000 series supervisor engine software Release 4.3(1a) and later
- ATM software Release 4.9(b) and later
- VTP Version 2

Note While VTP version 2 must be enabled on a Catalyst 5000 for Token Ring to function, do not use VTP to distribute VLAN configuration information between the switches. Configure the switches to operate in VTP transparent mode and manually configure the VLANs on each switch.

When you set up a LEC, follow these rules and recommendations:

- Make sure you properly configure the LECS and LES/BUS using the ATM module command-line interface (CLI) for each VLAN before creating a LEC. VTP does not set up the LECS or LES/BUS.
- In the set vlan interface configuration command, the vlan_num argument represents the VLAN number to configure, and the *vlan_name* argument is the name of the VLAN.
- The VLAN name must match the ELAN name and the ring number must match the local segment ID.

The **set vlan** interface configuration command assumes that any ring number you enter is in hexadecimal. Therefore, 0x12 or 12 is stored as the hexadecimal value 0x12. The **name** *elan_name* **local-seg-id** *segment_number*LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal. For example, to define a TrCRF with a ring number of 12 you could enter the **set vlan 12 name crf12 type trcrf ring 12 parent 100** interface configuration command or the **set vlan 12 name crf12 type trcrf ring 0x12 parent 100** interface configuration command.

When defining a corresponding LEC, you could enter name **crf12 local-seg-id 0x12** or **name crf12 local-seg-id 18** because 18 is the decimal equivalent of 0x12.

- Before you can create a LEC, the TrBRF and TrCRF to which it will be associated must exist.
- Do not create more than one LEC for each TrBRF per ATM module.

While you can have only one LEC per TrBRF per module, you can have more than one module installed. This allows you to have more than one LEC per TrBRF, which means the switch can participate in more than one ELAN. The ELANs, however, cannot be parallel or the Spanning-Tree Protocol will block one of the connections.

Note Configuring more than one LEC for a TrBRF on a single ATM module will adversely affect frame forwarding.

- Ensure that all-routes explorer (ARE) reduction is enabled (using the set tokenring reduction enable interface configuration command) on the Token Ring module.
- Do not configure parallel ELANs within a TrBRF (parallel ELANs are those ELANs that form a loop between switches).
- Do not create more than one LEC for each TrCRF per ATM module.

A TrCRF can include only one enabled LEC from any ATM module.

An ATM module LEC is assigned to a TrCRF to provide connectivity to the ATM network. In this sense, an ATM module is a logical port within the TrCRF. When assigning enabled LECs to TrCRFs, the enabled LECs of any one ATM expansion module should each be assigned to different TrCRFs.

- You can change all ELAN names with the exception of VLANs 1, 1003, or 1005 whose ELAN names must remain **default**, trcrf-default, and trbrf-default, respectively. You cannot override the ELAN name for VLAN 1, 1003, or 1005 by using the name elan_name parameter. You can assign all other VLANs any name.

When you enter the set vlan vlan_num [name vlan_name] interface configuration command in transparent mode and do not specify the optional **name** elan_name parameter, the software uses the names in the table below by default.

Table 25: Default VLAN ELAN Names

VLAN Number	VLAN Name
1	default
2...1002	VLAN0002 through VLAN1002
1003	trcrf-default
1004	VLAN1004
1005	trbrf-default

If you currently have a different ELAN name for VLAN 1 or VLAN 1003, you must change the ELAN name to default (for VLAN 1) or trcrf-default (for VLAN 1003) in the LECS database. The following example shows an LECS database configuration that specifies **marktng** as the ELAN name for VLAN 1003:

```
lane database test
name marktng server-atm-address 47.00918100000000061705B8301.00400B020011.01
```

```
!
interface ATM0
no ip address
no ip route-cache
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
lane config auto-config-atm-address
lane config database test
!
interface ATM0.1 multipoint
no ip route-cache
lane server-bus tokenring marktng
lane client tokenring 1003 marktng
```

You must change the ELAN name for VLAN 1003 from marktng to trcrf-default in the second and last lines of the display, as follows:

```
lane database test
name default server-atm-address 47.00918100000000061705B8301.00400B020011.01
!
interface ATM0
no ip address
no ip route-cache
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
lane config auto-config-atm-address
lane config database test
!
interface ATM0.1 multipoint
no ip route-cache
lane server-bus tokenring default
lane client tokenring 1003 trcrf-default
```

Creating a Token Ring VLAN

With Token Ring, to successfully route packets between ELANs, you can only set up one LEC for each TrBRF on an ATM module. For multiple ELANs with the same TrBRF to route packets, they must be configured on either separate ATM modules or connected via an external device.

If the TrBRF and TrCRF for which you are creating a LEC do not already exist, create the Token Ring VLANs by using the following commands beginning in privileged EXEC mode:

SUMMARY STEPS

1. Console> (enable) **set vlan***vlan_num* [**name***name*] **type trbrf** [**state** {**active** | **suspend**}] [**mtu***mtu*] **bridge***bridge_number* [**stp** {**ieee** | **ibm** | **auto**}]
2. Console> (enable) **set vlan***vlan_num* [**name***name*] **type trcrf** [**state** {**active** | **suspend**}] [**mtu***mtu*] **ring***ring_number***parent***vlan_num* [**mode** {**srt** | **srb**}] [**backupcrf** {**off** | **on**}] [**aremaxhop***hopcount*] [**stemaxhop***hopcount*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Console> (enable) **set vlan***vlan_num* [**name***name*] **type trbrf** [**state** {**active** | **suspend**}] [**mtu***mtu*] **bridge***bridge_number* [**stp** {**ieee** | **ibm** | **auto**}]	From the supervisor module, defines the TrBRF that you will associate to TrCRF as a parent

	Command or Action	Purpose
Step 2	Console> (enable) **set vlan***vlan_num* [**name***name*] **type trcrf** [**state** {**active** | **suspend**}] [**mtu***mtu*] **ring***ring_number***parent***vlan_num* [**mode** {**srt** | **srb**}] [**backupcrf** {**off** | **on**}] [**aremaxhop***hopcount*] [**stemaxhop***hopcount*]	From the supervisor module, defines the TrCRF for which you are creating a LEC.

Setting Up the Token Ring VLAN on a LEC

To set up the LEC for the Token Ring VLAN and corresponding ELAN, use the following commands on the ATM module beginning in global configuration mode:

SUMMARY STEPS

1. ATM(config)# **interface atm***number* [**.***subinterface-number*]
2. ATM(config-if)# **lane client tokenring vlan_id**[*elan-name1*]
3. ATM(config-if)# **exit**
4. ATM(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM(config)# **interface atm***number* [**.***subinterface-number*]	Specifies the subinterface for an ELAN on this switch and enters interface configuration mode.
Step 2	ATM(config-if)# **lane client tokenring vlan_id**[*elan-name1*]	Creates a LEC for the first ELAN and specifies the VLAN number and the ELAN name to which to bind the LEC.
Step 3	ATM(config-if)# **exit**	Exits configuration mode.
Step 4	ATM(config)# **copy running-config startup-config**	Saves the configuration.

Configuring Redundant LANE Services

The LANE protocol does not specify where any of the ELAN server entities should be located, but for the purpose of reliability and performance, Cisco implements these server components on its routers and LAN switches.

With Phase I LANE, only one LECS, capable of serving multiple ELANs, and only one LES per ELAN could exist for an ATM cloud. The Phase I LANE protocol did not allow for multiple LESs within an ELAN. Therefore, these components represented both single points of failure and potential bottlenecks for LANE service.

LANE LES/BUS and LECS redundancy corrects these limitations by allowing you to configure redundant LES/BUSs so that the LECs in an ELAN can automatically switch to a backup LES if the primary LES fails. The priority of the LES/BUS pairs is established by the order in which they are entered in the LECS database. LANE LES/BUS and LECS redundancy is always enabled. You can use this redundancy feature by configuring multiple servers.

LES/BUS and LECS redundancy works only with Cisco LECS and LES combinations. Third-party LANE server components continue to interoperate with the LECS and LES/BUS function of Cisco routers and switches, but cannot take advantage of the redundancy features.

The following servers are single points of failure in the ATM LANE system:

- LECS (configuration server)
- LES (ELAN server)
- BUS

LES/BUS and LECS redundancy eliminates these single points of failure.

Enabling Redundant LECSs

To enable redundant LECSs, enter the multiple LECS addresses to the end ATM switches, which are used as central locations for the list of LECS addresses. After entering the LECS addresses, LANE components connected to the switches can obtain the global list of LECS addresses.

Note To configure LES/BUS and LECS redundancy, you must enable multiple, redundant, and standby LECSs and multiple, redundant, and standby LES/BUSs. The LES/BUS and LEC redundancy configuration procedure guards against failure on hardware on which LANE components are running, including all Catalyst 5000 series switches. The configuration procedure is not effective for ATM network switch failures.

To enable LES/BUS and LEC redundancy, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Switch(config)# **atm lecs-address***address*
2. ATM(config)# **name elan-name server-atm-address les-address**[**index** *n*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Switch(config)# **atm lecs-address***address*	Allows you to enter the multiple LECS addresses on the ATM switch.
Step 2	ATM(config)# **name elan-name server-atm-address les-address**[**index** *n*]	Specifies redundant LES/BUSs on the ATM module. Enter the command for each LES address on the ELAN. The index determines the priority; 0 is the highest priority.

Enabling ILMI Keepalive Timeout

If enabled, ILMI sends keepalive messages on an ongoing basis on the active physical (PHY) to the switch, and the switch responds. If the response is not obtained for the last four polls, the ILMI timer times out and the Dual PHY changes from active PHY to backup PHY. This feature is useful only if the two PHYs are connected to two different switches.

By default, this feature is disabled. To enable it, start a session to the ATM module (using the **session** command), and then enter the following commands:

```
ATM> enable
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0
ATM(config-if)# atm ilmi-keepalive 4
ATM(config-if)# end
ATM#
```

These commands enable the transmission of ILMI keepalive messages and set the time between ILMI keepalive messages to 4 seconds.

Using UNI 3.1 Signalling Support

The ATM LANE Dual PHY module supports backward compatibility with ATM switches for UNI version 3.1. On startup, ILMI negotiates between UNI versions 3.0 and 3.1, which requires no configuration. If the ILMI link autodetermination is enabled on the interface, the router or switch accepts the UNI version returned by ILMI. If the ILMI link autodetermination is unsuccessful or if ILMI is disabled, the UNI version defaults to 3.0. You can override the version number by entering the **atm uni-version** command. If ILMI is enabled when you enter the no version of the command, the UNI version is set to the version returned by ILMI and the link autodetermination is successful. Otherwise, the version reverts to 3.0. Enter the no atm uni-version command to override the UNI version.

Note Each ELAN is a separate subnetwork.

Configuring Fast SSRP for Redundant LANE Services

With FSSRP, you can configure redundant LES/BUS pairs for each ELAN. With FSSRP, which differs from the previously implemented SSRP, all configured LESs of an ELAN are active which means FSSRP-aware redundant LES/BUS pairs can accept join requests from any FSSRP-aware client.

LECs that are FSSRP aware have VCs established to every single LES/BUS in the ELAN. Because VC connections already exist between all LECs and LES/BUS pairs in the ELAN, the LECs can switch over to another LES/BUS pair without any noticeable delay should a failure occur.

When you configure more than one LES/BUS pair for an ELAN, one LES/BUS takes precedence over others based on the order in which they are entered into the LECS database.

> **Note** Redundant LES/BUS pairs for a single ELAN should be configured on different ATM LANE modules in the LANE network for maximum fault tolerance.

Configuring redundant LES/BUS pairs for an ELAN is a two-part process:

- You must first configure the redundant LES/BUS pairs on subinterfaces for that ELAN.
- You must then enter the ATM addresses of the redundant LES/BUS pairs into the LECS database for the ELAN.

To configure the LES/BUS pairs, use the following commands beginning in privileged EXEC mode:

SUMMARY STEPS

1. ATM# **configure terminal**
2. ATM (config)# **interface atm0**
3. ATM (config-subif)# **lane fssrp**
4. ATM (config-subif)# **interface atm 0.** *subinterface-number*
5. ATM (config-subif)# **lane server-bus tokenring***elan-name*
6. Repeat Steps 2 and 3 for all LES/BUSs you want to configure on this ATM module.
7. ATM (config-subif)# **Ctrl-Z**
8. ATM# **show lane server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM# **configure terminal**	Enters global configuration mode.
Step 2	ATM (config)# **interface atm0**	Specifies the major interface and enters subinterface configuration mode.
Step 3	ATM (config-subif)# **lane fssrp**	Enables FSSRP on the major interface
Step 4	ATM (config-subif)# **interface atm 0.** *subinterface-number*	Specifies the subinterface for the first ELAN.
Step 5	ATM (config-subif)# **lane server-bus tokenring***elan-name*	Enables the LES/BUS for an ELAN on the subinterface (you cannot configure more than one LES/BUS per subinterface).
Step 6	Repeat Steps 2 and 3 for all LES/BUSs you want to configure on this ATM module.	
Step 7	ATM (config-subif)# **Ctrl-Z**	Exits subinterface configuration mode.
Step 8	ATM# **show lane server**	Verifies the LES/BUS configuration.

Configuring Fast SSRP for Redundant LANE Services

> **Note** The LES/BUSs are not fully operational until one or more LECs are configured and the LECS database is configured and bound to the ATM module interface.

This example shows how to specify the LES/BUS for an ELAN and verify the configuration

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0.1
ATM(config-subif)# lane server-bus tokenring default
ATM(config-subif)# interface atm0.2
ATM(config-subif)# lane server-bus tokenring Eng_ELAN
ATM(config-subif)# ^Z
ATM# show lane server
LE Server ATM0.1  ELAN name: default  Admin: up  State: operational
type: tokenring        Max Frame Size: 4472
ATM address: 47.00918100000000E04FACB401.00100DAACC41.01
LECS usef: 47.007900000000000000000000.00A03E000001.00 NOT yet connected
LE Server ATM0.2  ELAN name: Eng_ELAN  Admin: up  State: operational
type: tokenring        Max Frame Size: 4472
ATM address: 47.00918100000000E04FACB401.00100DAACC41.02
LECS usef: 47.007900000000000000000000.00A03E000001.00 NOT yet connected
```

To add the redundant LES/BUS pairs to the LECS, use the following commands beginning in privileged EXEC configuration mode

SUMMARY STEPS

1. ATM# **show lane server**
2. ATM# **configure terminal**
3. ATM (config)# **lane database** *database-name*
4. ATM (lane-config-database)# **name** *elan-name***server-atm-address***atm-address*
5. ATM (lane-config-database)# **default-name***elan-name*
6. ATM (lane-config-database)# **Ctrl-Z**
7. ATM# **show lane database**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ATM# **show lane server**	Displays the ATM address of the LES/BUS for the ELAN.
Step 2	ATM# **configure terminal**	Enters global configuration mode.
Step 3	ATM (config)# **lane database** *database-name*	Enters database configuration mode, specifying a LANE database name.
Step 4	ATM (lane-config-database)# **name** *elan-name***server-atm-address***atm-address*	Binds the name of the ELAN to the ATM addresses of the LES/BUS pairs in the order you want the services to fail over.

	Command or Action	Purpose
Step 5	ATM (lane-config-database)# **default-name***elan-name*	In the configuration database, provides a default name of the ELAN.
Step 6	ATM (lane-config-database)# **Ctrl-Z**	Exits from database configuration mode.
Step 7	ATM# **show lane database**	Displays the LECS database configuration so that you can verify your changes.

What to Do Next

This example shows how to display the ATM address of the LES/BUS of the default ELAN, how to configure the LECS database for the default ELAN, and how to verify the configuration:

```
ATM# show lane server
LE Server ATM0.1  ELAN name: default  Admin: up  State: operational
type: ethernet         Max Frame Size: 1516
ATM address: 47.00918100000000E04FACB401.00100DAACC41.01
LECS usef: 47.007900000000000000000000.00A03E000001.00 NOT yet connected

ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# lane database LANE_Backbone
ATM(lane-config-database)# name default server-atm-address
 47.00918100000000E04FACB401.00100DAACC41.01
ATM(lane-config-database)# default-name default
ATM(lane-config-database)# ^Z
ATM# show lane database

LANE Config Server database table 'LANE_Backbone'
default elan: default
elan 'default': un-restricted
  server 47.00918100000000E04FACB401.00100DAACC41.01 (prio 0)
```

Verifying the LANE Setup

Once you have set up the LECs on the subinterfaces of an ATM module, you can display their ATM addresses by using the following command in privileged EXEC mode:

Command	Purpose
`Router#` **show lane**	Displays the LES, BUS, and LEC ATM addresses.

The command output shows all the subinterfaces configured for LANE. For each subinterface, the command displays and labels the ATM addresses that belong to the LES, BUS, and the LEC.

When you look at each ATM address, confirm the following items:

- The prefix is the one you set up on the switch.
- The end-system identifier field reflects the base address of the pool of MAC addresses assigned to the ATM interface plus a value that represents the specific LANE component.

- The selector byte is the same number as the subinterface (converted to hexadecimal).

Enter the **show lane** EXEC command on each Catalyst 5000 series switch to verify the LANE setup before you set up the LECs on the next Catalyst 5000 series switch. Print the display or make a note of these ATM addresses so that you can use it when you set up the LECS database. At this point in the configuration process, the LECs are not normally operational.

Monitoring and Maintaining LANE Components

After configuring LANE components on an interface or any of its subinterfaces, you can display their status on a specified subinterface or on an ELAN. To show LANE information, issue the following commands in privileged EXEC mode:

Command	Purpose
Router# **show lane** [**interface atm 0** [*subinterface-number* | **name** *elan-name*]] [**brief**]	Displays the global and per-VCC LANE information for all the LANE components and ELANs configured on an interface or any of its subinterfaces.
Router# **show lane bus** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for the BUS configured on any subinterface or ELAN.
Router# **show lane client** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for all LECs configured on any subinterface or ELAN.
Router# **show lane config** [**interface atm 0**]	Displays the global and per-VCC LANE information for the LECS configured on any interface.
Router# **show lane database** [*database-name*]	Displays the LECS database.
Router# **show lane le-arp** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*]	Displays the LE_ARP table of the LECs configured on the specified subinterface or ELAN.
Router# **show lane server** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for the LES configured on a specified subinterface or ELAN.

Note For descriptions of the output displayed by the commands listed above, see the description of the command documented in the *Cisco IOS Switching Services Command Reference* .

Token Ring LANE Configuration Example

This section provides a configuration example composed of two Catalyst 5000 series switches and a Cisco LightStream 1010 ATM switch as shown in the figure below.

Example Assumptions

For the example in the "Token Ring LANE Configuration Example," the following assumptions apply:

- Catalyst 5000 series switches with the ATM modules installed are running ATM software Release 4.9b or later.
- Catalyst 5000 series switch 1 runs the LES/BUS and LECS on interface **atm0** and the LEC on interface **atm0.1**.
- Catalyst 5000 series switch 2 runs LEC on interface **atm0.1**.
- The ATM module is installed in slot 4 of both Catalyst 5000 series switches.
- You can change the ELAN name by entering the set vlan *vlan_num* [**name** *vlan_name*] command.
- The ELAN on the switches is essentially a new TrCRF. The ELAN name is crf112 and the VLAN ID is 112.
- The parent TrBRF to the TrCRF 112 is brf400 (VLAN ID 400).

Configuring the TrCRF Example

To define the TrCRF, perform the following tasks:

SUMMARY STEPS

1. At the enable prompt, enter the following command:
2. To verify the configuration of the new VLAN, enter the **show vlan**command.

DETAILED STEPS

Step 1 At the enable prompt, enter the following command:

Example:

```
Console> (enable) set vlan 112 name crf112 type trcrf ring 112 parent 400 mode srb
```

Step 2 To verify the configuration of the new VLAN, enter the **show vlan**command.
The output indicates that crf112 has been added and that brf400 is its parent:

Example:

```
Console> (enable) show vlan 112
VLAN Name                             Status    Mod/Ports, Vlans
---- -------------------------------- --------- ----------------------------
112  crf112                           active
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
112  trcrf 100112     4472  400    0x112  -      -    srb      0      0
VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
112  7       7       off
Console> (enable)
```

Configuring the LES BUS and the LEC Example

To configure the LES/BUS and LEC, perform the following tasks:

SUMMARY STEPS

1. Set up the prefix of the ATM NSAP address for the switch.
2. Start a session to the ATM module by entering the session 4 interface configuration command. You see the following display:
3. Obtain the addresses of the LES/BUS for later use by entering the **enable** router configuration command (to enable configuration mode) and the show lane default-atm-addresses EXEC command at the ATM prompt. You see the following display:
4. Using the LECS address obtained in Step 3, set the address of the default LECS in the LightStream 1010 switch by entering the configure terminal and atm lecs-address-default commands on the console of the LightStream 1010 switch. You see the following display:
5. Save the configuration to NVRAM by entering the **write memory** command, as follows:
6. Start a LES/BUS pair on Catalyst 5000 series switch 1 by entering the interface atm0 and the lane server-bus tokenring commands in global configuration mode. On the console of Catalyst 5000 series switch 1, enter the following commands:
7. Save the configuration in NVRAM entering the **write memory** command, as follows:
8. Set up the LECS database on the Catalyst 5000 series switch 1.
9. Save the configuration in NVRAM by entering the write memory command, as follows:
10. Start and bind the LECS on the Catalyst 5000 series switch 1 by entering the interface atm0, the lane config database *database_name* interface configuration command, and the lane config auto-config-atm-address interface configuration commands at the ATM prompt. You see the following display:
11. Save the configuration in NVRAM by entering the **write memory** command, as follows:
12. Start the LEC on the Catalyst 5000 series switches 1 and 2 by entering the interface atm0.1 command and the lane client tokenring 112 crf112 interface configuration command in configuration mode on the consoles of switches 1 and 2. The interface on which the LEC is configured is *atm0.1*. The ELAN name is default, and it is configured to emulate Token Ring. You see the following display:
13. Save the configuration in NVRAM by entering the write memory command, as follows:

DETAILED STEPS

Step 1 Set up the prefix of the ATM NSAP address for the switch.
The LightStream 1010 ATM switch provides a default prefix.

Step 2 Start a session to the ATM module by entering the session 4 interface configuration command. You see the following display:

Example:

```
Console> session 4
Trying ATM-4...
Connected to ATM-4.
Escape character is '^]'.
ATM>
```

Step 3 Obtain the addresses of the LES/BUS for later use by entering the **enable** router configuration command (to enable configuration mode) and the show lane default-atm-addresses EXEC command at the ATM prompt. You see the following display:

Example:

```
ATM> enable
ATM#
ATM# show lane default-atm-addresses interface atm0
interface ATM0:
LANE Client:        47.00918100000000061705b7701.00400BFF0010.**
LANE Server:        47.00918100000000061705b7701.00400BFF0011.**
LANE Bus:           47.00918100000000061705b7701.00400BFF0012.**
LANE Config Server: 47.00918100000000061705b7701.00400BFF0013.00
ATM#
```

The two asterisks (**) represent the subinterface number byte in hexadecimal.

Step 4 Using the LECS address obtained in Step 3, set the address of the default LECS in the LightStream 1010 switch by entering the configure terminal and atm lecs-address-default commands on the console of the LightStream 1010 switch. You see the following display:

Example:

```
Switch> enable
Switch#
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# atm lecs-address-default 47.00918100000000061705b7701.00400BFF0013.00 1
Switch(config)# end
Switch#
```

The commands shown in this step configure the address of the LECS in the switch. The LECS ATM NSAP address is 47.00918100000000061705b7701.00400BFF0013.00. The sequence number of this LECS address, which is 1, means it is the first LECS in this switch.

Step 5 Save the configuration to NVRAM by entering the **write memory** command, as follows:

Example:

```
ATM# write memory
```

Step 6 Start a LES/BUS pair on Catalyst 5000 series switch 1 by entering the interface atm0 and the lane server-bus tokenring commands in global configuration mode. On the console of Catalyst 5000 series switch 1, enter the following commands:

Example:

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0
ATM(config-subif)# lane server-bus tokenring crf112
ATM(config-subif)# end
ATM#
```

The commands shown in this step start a LES/BUS pair and assign the ATM 0 interface to crf112. The ELAN name is **crf112**, and the interface on which this LES/BUS pair is configured is **atm0**. The ELAN name must be the same as the VLAN name assigned to the TrCRF.

Step 7 Save the configuration in NVRAM entering the **write memory** command, as follows:

Example:

```
ATM# write memory
```

Step 8 Set up the LECS database on the Catalyst 5000 series switch 1.
Enter the LES address obtained in Step 3 and replace the ** with the subinterface number of the interface on which the LES/BUS is to be configured. In this example, that number is 00. Enter the lane database *database_name*interface configuration command, the name *elan_name* server-atm-address *atm_address* LANE database configuration command, the name elan_name local-seg-id segment_number LANE database configuration command, and the default-name *elan_name* commands at the ATM prompt. You see the following display:

Example:

```
ATM# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# lane database test
ATM(lane-config-database)# name trcf-default server-atm-address
                             47.00918100000000061705b7701.00400BFF0011.00
ATM (lane-config-database) name crf112 local-seg-id 0x112
ATM(lane-config-database)# default-name crf112
ATM(lane-config-database)# exit
ATM#
```

The commands shown in this step create the LECS database. The database name is *test*. The ELAN name is **crf112**. The ELAN segment number is 112 . The LES ATM NSAP address is 47.00918100000000061705b7701.00400BFF0011.00 .

The segment number you specify for **local-seg-id** keyword must be identical to the ring number of the TrCRF. The **set vlan**command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal.

Step 9 Save the configuration in NVRAM by entering the write memory command, as follows:

Example:

```
ATM# write memory
```

Step 10 Start and bind the LECS on the Catalyst 5000 series switch 1 by entering the interface atm0, the lane config database *database_name* interface configuration command, and the lane config auto-config-atm-address interface configuration commands at the ATM prompt. You see the following display:

Example:

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0
ATM(config-if)# lane config database test
ATM(config-if)# lane config auto-config-atm-address
ATM(config-if)# end
ATM#
```

The commands shown in this step start the LECS. The database to use is *test*. The interface on which the LECS is configured is *atm0*.

Step 11 Save the configuration in NVRAM by entering the **write memory** command, as follows:

Example:

```
ATM# write memory
```

Step 12 Start the LEC on the Catalyst 5000 series switches 1 and 2 by entering the interface atm0.1 command and the lane client tokenring 112 crf112 interface configuration command in configuration mode on the consoles of switches 1 and 2. The interface on which the LEC is configured is *atm0.1*. The ELAN name is default, and it is configured to emulate Token Ring. You see the following display:

Example:

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0.1
ATM(config-subif)# lane client tokenring 112 crf112
ATM(config-subif)# end
ATM#
```

Step 13 Save the configuration in NVRAM by entering the write memory command, as follows:

Example:

```
ATM# write memory
```

CHAPTER 24

SNMP Trap Support for the Virtual Switch Interface Master MIB

This feature module explains how to use the virtual switch interface (VSI) Master MIB to monitor and manage ATM switches that are connected to routers through the virtual switch interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SNMP Trap Support for the VSI Master MIB

Memory Requirements

- The VSI Master MIB requires 75K of space.
- The runtime dynamic random-access memory (DRAM) is approximately 5K times the number of logical/slave interfaces the VSI controller manages.

Performance

The VSI cross-connect error messages can be invoked hundreds of times every second. To prevent a performance impact on the label switch controller (LSC), enable rate-limiting to control the amount of traffic that passes into or out of an interface.

Restrictions for SNMP Trap Support for the VSI Master MIB

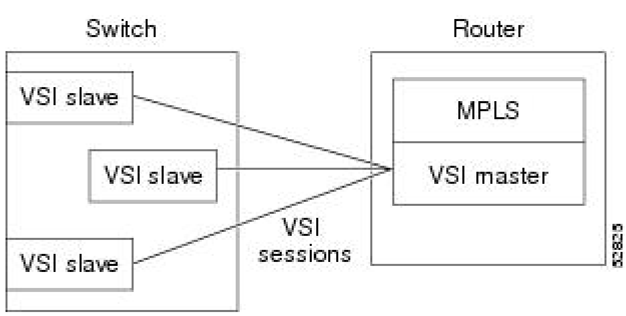
The VSI Master MIB is for ATM-LSRs running Multiprotocol Label Switching (MPLS).

Information About SNMP Trap Support for the VSI Master MIB

VSI Master and Slave

The VSI master is a software module that resides on a router. The VSI master enables an application to control an ATM switch that is connected to the router. The VSI protocol runs between the VSI master and a VSI slave. The VSI master can communicate with more than one slave across a control interface that connects the router to the switch. Each master/slave connection is called a VSI session. The figure below illustrates VSI sessions between a VSI master and slaves.

Figure 42: VSI Master and VSI Slaves



VSI Components That You Can Monitor with the VSI Master MIB

The VSI Master MIB allows you to monitor the operation of the switch. It also displays the results of the operations. Specifically, the VSI Master MIB allows you to monitor:

- Connections between the router and the controlled switch.
- The status of the interfaces in the switch
- Virtual circuits (VCs) that are maintained across the interfaces.

MIB Traps

The VSI Master MIB allows you to enable traps on the following components:

- Controllers--When VSI controllers are added or deleted
- VSI sessions--When VSI sessions are established or disconnected
- Logical interfaces--When logical interfaces become active or fail.
- Cross-connects--When a cross-connect cannot be established.
- Virtual circuits--When cross-connect resource thresholds are below configured thresholds.

MIB Objects

The following is a partial list of the supported MIB objects.

Controllers

You can obtain the following information about the controller:

- Controller identifier
- Number of cross-connects maintained in the switch
- Protocol version
- Controller interface index
- Slave interface identifiers
- Controller IP address

Sessions

You can obtain the following information about the VSI sessions:

- Virtual path identifiers (VPIs) for session connections
- Virtual circuit identifiers (VCIs) for the sessions
- Switch identifier
- Switch name

- Session state
- Protocol session monitoring

Logical Interfaces

Logical interfaces represent external interfaces that are available for connections. When you pair two external interfaces (represented by two logical interfaces), they provide a physical path through the switch. These physical paths support cross-connects. You can gather the following information about each logical interface:

- Interface name
- Operational state
- Administrative state
- Operational statistics
- Cross-connect usage
- Cross-connect availability
- Cross-connect capacity
- Interface capabilities
- VC ranges
- Interface index
- IP address

Cross-Connects

Cross-connects are virtual links across two interfaces. The participating interfaces that support these links are listed in the MIB's vsiLogicalIfTable entries. You can gather the following information about the cross-connects:

- Interface associations
- State
- Identifiers
- VPI/VCI identifiers for supporting interfaces

How to Configure SNMP Trap Support for the VSI Master MIB

Enabling the SNMP Agent

The SNMP agent for the VSI Master MIB is disabled by default. To enable the SNMP agent, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **show running-configuration**
3. **configure terminal**
4. snmp-server community *string* RO
5. **exit**
6. write memory

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-configuration** **Example:** `Router# show running-configuration`	Displays the running configuration to see if the SNMP agent is already running. If no SNMP information is present, continue with the steps below. If any SNMP commands are listed, you can modify them or leave them as they are.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	snmp-server community *string* RO **Example:** `router(config)# snmp-server community` *string* `RO`	Enables the read-only community string, where *string* is the read-only community string.
Step 5	**exit** **Example:** `router(config)# exit`	Exits the configuration mode and returns to the main prompt.
Step 6	write memory **Example:** `router# write memory`	Writes the modified configuration to nonvolatile memory (NVRAM) so that the settings stay permanently.

Verifying That the SNMP Agent Has Been Enabled

To verify that the SNMP agent has been enabled, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **show running-configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-configuration** **Example:** `Router# show running-configuration`	Displays the running configuration to see if the SNMP agent is already running. If you see any "snmp-server" statements, SNMP has been enabled on the router.

Enabling Traps

SNMP notifications can be sent as traps or inform requests. A trap is an unsolicited message sent by an SNMP agent to an SNMP manager, indicating that some event has occurred. You can enable SNMP traps for the VSI Master MIB through the command line interface (CLI) or through an SNMP MIB object. The following sections explain these options.

Enabling the VSI Master MIB Traps by Using Commands

To enable SNMP traps, use the snmp-server enable traps command. An SNMP agent can be configured to send traps when one of the VSI Master MIB objects changes.

The table below lists the CLI commands for enabling traps of specific VSI components.

Table 26: CLI Commands that Control the Type of Traps You Receive

To Receive Traps About	Use This Command
All components	**snmp server enable traps vsimaster**
Controllers being added or deleted	**snmp server enable traps vsimaster controller**

To Receive Traps About	Use This Command
Sessions that connect or disconnect	**snmp server enable traps vsimaster session**
Logical interfaces that connect or disconnect	**snmp server enable traps vsimaster logical-interface**
Cross-connects that fail	**snmp server enable traps vsimaster cross-connect**

To enable VSI Master MIB traps to be sent from the agent to the manager, perform the following tasks in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps vsimaster**
4. **snmp-server host** *hostname* *community-string* **vsimaster**
5. **exit**

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	**snmp-server enable traps vsimaster** **Example:** `router(config)# snmp-server enable traps vsimaster`	Enables the router to send VSI Master MIB traps.
Step 4	**snmp-server host** *hostname* *community-string* **vsimaster** **Example:** `router(config)# snmp-server host cisco.com restricted vsimaster`	Specifies the recipient of the trap message

	Command or Action	Purpose
Step 5	**exit** **Example:** `router(config)# exit`	Exits the configuration mode and returns to the main prompt.

Enabling the VSI Master MIB Traps by Using SNMP MIB Objects

You can also use MIB objects to specify which VSI components should send traps. To enable all VSI Master traps, use the vsiVSITrapEnable MIB object.

Controller Traps

To enable traps about the status of the controller, use the vsiControllerTrapEnable MIB object. The table below lists the MIB objects that are specific to the controller.

Table 27: Controller Traps

To Receive Traps When	Use This MIB Object
A controller is added	vsiControllerAdded
A controller is deleted	vsiControllerDeleted

VSI Session Traps

To enable traps about the status of the VSI sessions, use the vsiSessionTrapEnable MIB object. The table below lists the MIB objects that are specific to the VSI sessions.

Table 28: VSI Session Traps

To Receive Traps When	Use This MIB Object
A VSI session is established	vsiSessionUp
A VSI session is disconnected	vsiSessionDown

Logical Interfaces

To enable traps about the status of the logical interfaces, use the vsiLogicalIfTrapEnable MIB object. The table below lists the MIB objects that are specific to the logical interfaces.

Table 29: Logical Interface Traps

To Receive Traps When	Use This MIB Object
A logical interface is active	vsiLogicalIfUp
A logical interface fails	vsiLogicalIfDown

Cross-Connects

To enable traps about the status of the cross-connects, use the vsiXCTrapEnable MIB object. The table below lists the MIB objects that are specific to the cross-connects.

Table 30: Cross-Connect Traps

To Receive Traps When	Use This MIB Object
A cross-connect cannot be established	vsiXCFailed
The LCN resources drop, possibly causing resource exhaustion.	vsiLcnExhaustionNotice

Setting Thresholds for Cross-Connects

When cross-connects on XtagATM interfaces are created or deleted, a counter keeps a tally of the available logical channel number (LCN) resources. If the LCN resources become too low, the MIB sends messages to alert you of the possibility of resource exhaustion.

You must first set the warning and alarm thresholds for the number of LCNs. To set the warning threshold, use the vsiAvailableChnlWarnThreshold MIB object. To set the alarm threshold, use the vsiAvailableChnlAlarmThreshold MIB object. The following list explains the usage guidelines of these MIB objects:

- The threshold range is 1 to 100.
- The warning threshold value must be greater than or equal to the value of the alarm threshold. Likewise, the alarm threshold value must be less than or equal to the value of the warning threshold.
- If you only set one threshold, the MIB automatically sets the other threshold value to the same value as the threshold value you set.
- By default, the threshold functionality is disabled.

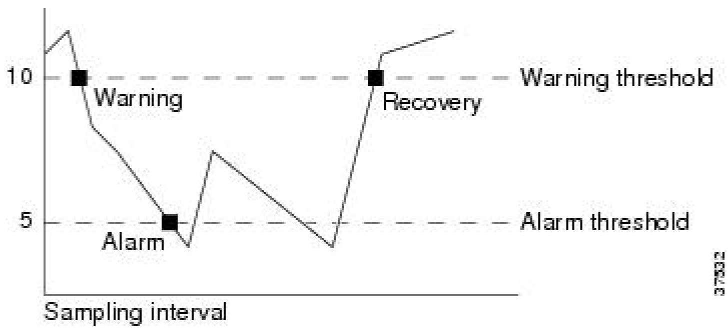
The following list explains the conditions under which warnings, alarms, and other messages are sent. The figure below illustrates the thresholds.

- If the number of LCNs falls below the the warning threshold, a warning is sent. This message indicates that the potential for resource exhaustion is possible.

- If the number of LCNs falls below the alarm threshold, an alarm is generated. This message indicates that the potential for resource exhaustion is imminent. If resource exhaustion occurs, cross-connects cannot be set up.
- If the number of LCNs returns to above the warning threshold, a recovery message is generated. This message means that the potential for resource exhaustion no longer exists.
- If the number of LCNs never crosses any threshold during the polling period, a normal message is generated.

To prevent an overwhelming number of warnings or alarms from being generated during a sampling period, only one warning or alarm is generated when the number of LCNs falls below the threshold. The number of LCNs must return to normal before another warning or alarm is generated.

Figure 43: Warning and Alarm Thresholds



Note If XtagATM interfaces share resources, the LCN does not represent the actual amount of available resources. For example, the interfaces XtagATM1 and XtagATM2 share resources. If a cross-connect is set up on XtagATM1 but not on XtagATM2, XtagATM1 takes resources away from XtagATM2. When the VSI slave reports the available resources, it only reports on the resources for XtagATM1. The resources for XtagATM2 are not reported. This is because the VSI slave provides updates only when a cross-connect is set up or torn down or when the slave's resources are partitioned. Any interfaces that are not set up or torn down do not send updates. As a result, if XtagATM2 doesn't have enough resources in the resource pool, the problem does not get reported.

Configuration Examples for SNMP Trap Support for the VSI Master MIB

Enabling the SNMP Agent Example

In the following example, the SNMP agent is enabled.

```
snmp-server community
```

Enabling the SNMP Agent with a Community String Example

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string public.

```
snmp-server community public
```

Enabling the SNMP Agent with Read-Only Access to Access List Members Example

In the following example, read-only access is granted for all objects to members of access list 4 that specify a community string named comaccess. No other SNMP managers have access to any objects.

```
snmp-server community comaccess ro 4
```

Enabling Traps and Specifying the Trap Recipient Example

In the following example VSI Master MIB traps are sent to the host cisco.com. The community string is restricted. The first line enables the router to send VSI Master MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous snmp-server host commands for the host cisco.com.

```
snmp-server enable traps vsimaster
snmp-server host cisco.com restricted vsimaster
```

Additional References for ATM Multilink PPP Support on Multiple VCs

The following sections provide references related to the ATM Multilink PPP Support on Multiple VCs feature.

Related Documents

Related Topic	Document Title
QoS configuration tasks	*Cisco IOS Quality of Service Solutions Configuration Guide*
QoS commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
WAN configuration tasks	*Cisco IOS Wide-Area Networking Configuration Guide*

Related Topic	Document Title
WAN commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Wide-Area Networking Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1990	*The PPP Multilink Protocol (MP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SNMP Trap Support for the VSI Master MIB

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 31: Feature Information for SNMP Trap Support for the Virtual Switch Interface Master MIB

Feature Name	Releases	Feature Information
SNMP Trap Support for the Virtual Switch Interface Master MIB	12.2(2)T, 12.4(20)T	This feature module explains how to use the virtual switch interface (VSI) Master MIB to monitor and manage ATM switches that are connected to routers through the virtual switch interface. The following commands were introduced or modifief: **snmp-server community**, **snmp-server enable traps**, **snmp-server host**. Support was removed for this feature in Cisco IOS Release 12.4(20)T and later releases.

Glossary

cloning --Creating and configuring a virtual-access interface by applying a specific virtual template interface. The template is the source of the generic user information and router-dependent information. The result of cloning is a virtual-access interface configured with all the commands in the template.

LCP --Link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.

NAS --Network access server. A device providing local network access to users across a remote access network such as the Public Switched Telephone Network (PSTN).

PPP --Point-to-Point Protocol. A protocol that encapsulates network layer protocol information over point-to-point links. PPP is defined in RFC 1661.

PPPoA --PPP over ATM.

PPPoE --PPP over Ethernet.

precloning --Cloning a specified number of virtual-access interfaces from a virtual template at system startup or when the command is configured.

PVC --Permanent virtual circuit (or connection). Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.

VC --Virtual channel. Logical circuit created to ensure reliable communication between two network devices. A VC is defined by a VPI/VCI pair and can be either permanent (PVC) or switched (SVC).

virtual-access interface --Instance of a unique virtual interface that is created dynamically and exists temporarily. Virtual-access interfaces can be created and configured differently by different applications, such as virtual profiles and virtual private dialup networks. Virtual-access interfaces are cloned from virtual template interfaces.

virtual template interface --A logical interface configured with generic configuration information for a specific purpose or configuration common to specific users, plus router-dependent information. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual-access interfaces, as needed.

VPDN --virtual private dial-up network. A system that permits dial-in networks to exist remotely from home networks, while giving the appearance of being directly connected.

CHAPTER 25

VLAN 0 Priority Tagging Support

The VLAN 0 Priority Tagging Support feature enables 802.1Q Ethernet frames to be transmitted with the VLAN ID tag set to zero. These frames are called priority tagged frames. Setting the VLAN ID tag to zero allows the VLAN ID tag to be ignored and the Ethernet frame to be processed according to the priority configured in the 802.1P bits of the 802.1Q Ethernet frame header.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for VLAN 0 Priority Tagging Support

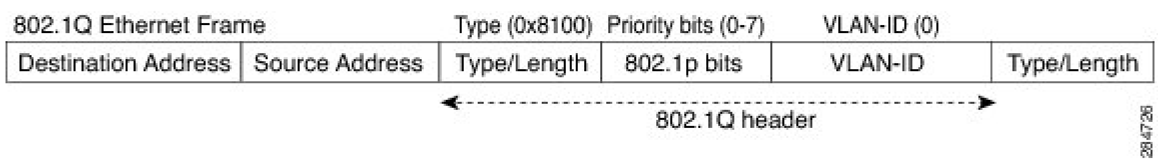
- QinQ is not supported with this feature.

Information About VLAN 0 Priority Tagging Support

802.1Q Tagging

The 802.1Q standard defines a system of VLAN tagging for Ethernet frames and also contains a provision for a quality of service (QoS) prioritization scheme known as 802.1P, which indicates the priority level of the frame. The 802.1Q standard adds this information to the Ethernet header, as shown in the figure below. The priority level values range from zero (best effort) to seven (highest). These values can be used to prioritize different classes of traffic such as voice and video. The VLAN ID tag specifies the VLAN to which the frame belongs. The priority bits define the priority with which the frames are processed.

Figure 44: 802.1Q Ethernet Frame



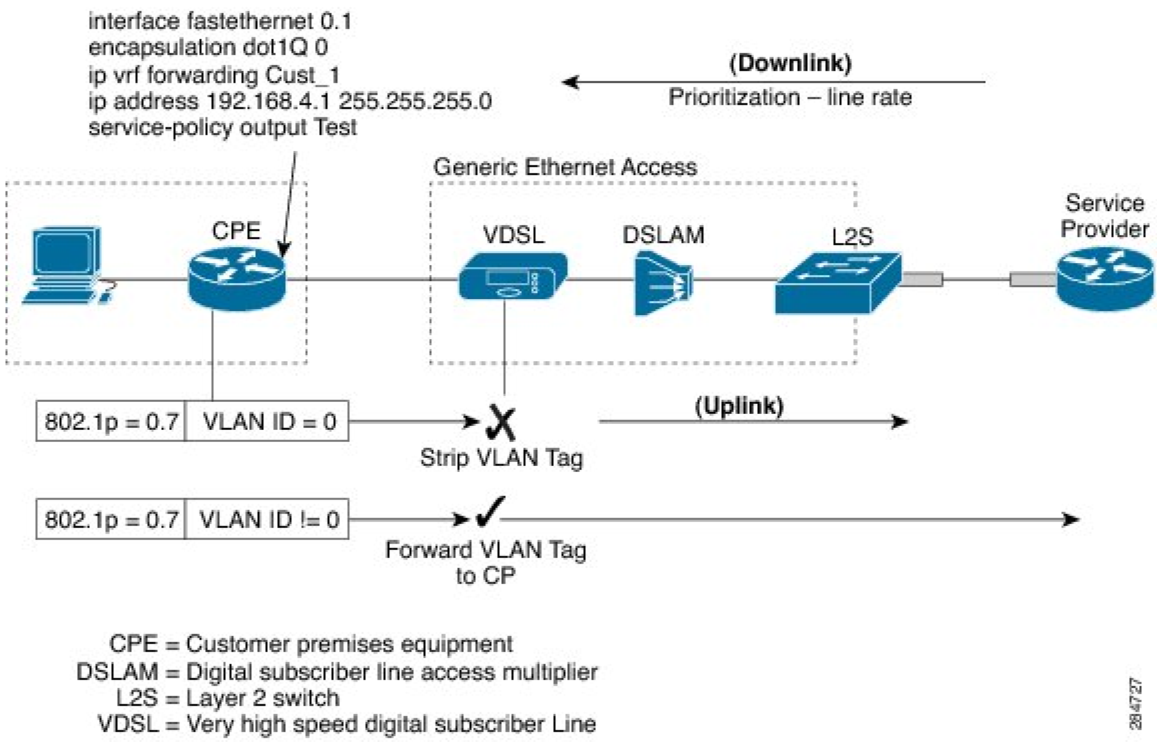
Native VLANs

When a particular VLAN ID is assigned as a native VLAN, frames that are sent from that native VLAN subinterface are not tagged. Similarly, any untagged frames received on that subinterface are associated with the native VLAN. A native VLAN sends only untagged frames, but can receive both tagged and untagged frames.

VLAN 0 Priority Tagging Overview

The VLAN 0 Priority Tagging feature is installed on the customer premises equipment (CPE). In the illustration below, the 802.1Q frames are sent in the upstream direction from the CPE to the internet service provider (ISP). The frames are transmitted with the 802.1Q VLAN tag set to zero and the 802.1P priority bits configured as per the priority with which the frames are to be processed. When these frames are received at the ISP end, the header is stripped off and the frame is processed as per the configuration of the 802.1P priority bits. If the VLAN ID has a nonzero value, the header is retained and the frame is transmitted to the specified VLAN subinterface. High priority frames are sent ahead of low priority frames, and this prioritization is weighted, that is, low priority traffic is not completely suppressed even if high priority traffic exceeds the line rate.

Figure 45: VLAN 0 Priority Tagging



The VLAN 0 Priority Tagging Support feature also allows VLAN 0 to be set as a native VLAN using the **encapsulation priority-tagged native** command. Setting the VLAN 0 subinterface as a native VLAN allows this subinterface to receive both tagged and untagged frames but transmit only untagged frames. The **encapsulation priority-tagged native tx-tagged** command configures the native VLAN with VLAN 0 to receive both tagged and untagged frames but to transmit only tagged frames.

How to Configure VLAN 0 Priority Tagging Support

Configuring VLAN 0 Priority Tagging

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **encapsulation priority-tagged**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Ethernet 0/0.1`	Configures an interface and enters subinterface configuration mode.
Step 4	**encapsulation priority-tagged** **Example:** `Device(config-subif)# encapsulation priority-tagged`	Sets the VLAN ID tag of the subinterface to zero.
Step 5	**end** **Example:** `Device(config-subif)# end`	Exits subinterface configuration mode and returns to privileged EXEC mode.

Configuring a VLAN 0 Subinterface as a Native VLAN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **encapsulation priority-tagged**
5. **encapsulation priority-tagged native**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Ethernet 0/0.1`	Configures an interface and enters subinterface configuration mode.
Step 4	**encapsulation priority-tagged** **Example:** `Device(config-subif)# encapsulation priority-tagged`	Sets the VLAN ID tag of the subinterface to zero.
Step 5	**encapsulation priority-tagged native** **Example:** `Device(config-subif)# encapsulation priority-tagged native`	Configures the priority-tagged subinterface as a native VLAN.
Step 6	**end** **Example:** `Device(config-subif)# end`	Exits subinterface configuration mode and returns to privileged EXEC mode.

Configuring Native VLAN to Transmit Tagged Frames

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **encapsulation priority-tagged**
5. **encapsulation priority-tagged native**
6. **encapsulation priority-tagged native tx-tagged**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Ethernet 0/0.1`	Configures an interface and enters subinterface configuration mode.
Step 4	**encapsulation priority-tagged** **Example:** `Device(config-subif)# encapsulation priority-tagged`	Sets the VLAN ID tag of the subinterface to zero.
Step 5	**encapsulation priority-tagged native** **Example:** `Device(config-subif)# encapsulation priority-tagged native`	Configures the priority tagged subinterface as a native VLAN.
Step 6	**encapsulation priority-tagged native tx-tagged** **Example:** `Device(config-subif)# encapsulation priority-tagged native tx-tagged`	Configures the priority tagged native VLAN interface to transmit tagged frames.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-subif)# end`	Exits subinterface configuration mode and returns to privileged EXEC mode.

Configuration Examples for VLAN 0 Priority Tagging Support

Example: Configuring a Priority Tagged Native VLAN Interface to Transmit Tagged Frames

```
Device> enable
Device# configure terminal
Device(config)# interface Ethernet 0/0.1
Device(config-subif)# encapsulation priority tagged
Device(config-subif)# encapsulation priority-tagged native
Device(config-subif)# encapsulation priority-tagged native tx-tagged
Device(config-subif)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ATM commands	Cisco IOS Asynchronous Transfer Mode Command Reference

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VLAN 0 Priority Tagging Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 32: Feature Information for VLAN 0 Priority Tagging Support

Feature Name	Releases	Feature Information
VLAN 0 Priority Tagging Support	15.2(3)T	The VLAN 0 Priority Tagging Support feature enables 802.1Q Ethernet frames to be transmitted with the VLAN ID tag set to zero. The following command was introduced or modifief: **encapsulation priority-tagged**.

CHAPTER 26

Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

The Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature allows 802.1Q tags to be transported over ATM permanent virtual circuits (PVC) used in Asymmetric Digital Subscriber Line 2+ (ADSL2+) uplinks. Additionally, 802.1P marking is allowed and is based on 802.1Q tagging.

Note Although this document uses the generic term ADSL, this feature requires an ADSL2+ uplink.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

- You must have a basic understanding of ATM, bridging, DHCP, and VLANs before configuring this feature.

Restrictions for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

- Supports only one bridged 802.1Q VLAN.
- Can be configured only on a point-to-point ATM subinterface.
- Uses ATM Adaptation Layer 5 Subnetwork Protocol Access Protocol (AAL5SNAP) encapsulation to enable the transport of an 802.1Q tag over an ATM PVC.

Information About Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Benefits of Preserve 802.1Q Tagging with 802.1P Marking

- CPE can carry traffic with 802.1P-marked provider-specific 802.1Q tags.
- Voice, video, and data services can be deployed at customer premises. This service combination offers a real-time channel dedicated to VoIP traffic and a second channel that delivers best-effort Internet service.
- All traffic is marked with an 802.1P marking which is implemented using VLAN-based service differentiation.

Note Support for PVCs configured with Route-Bridge Encapsulation (RBE) was introduced with CSCtt22809.

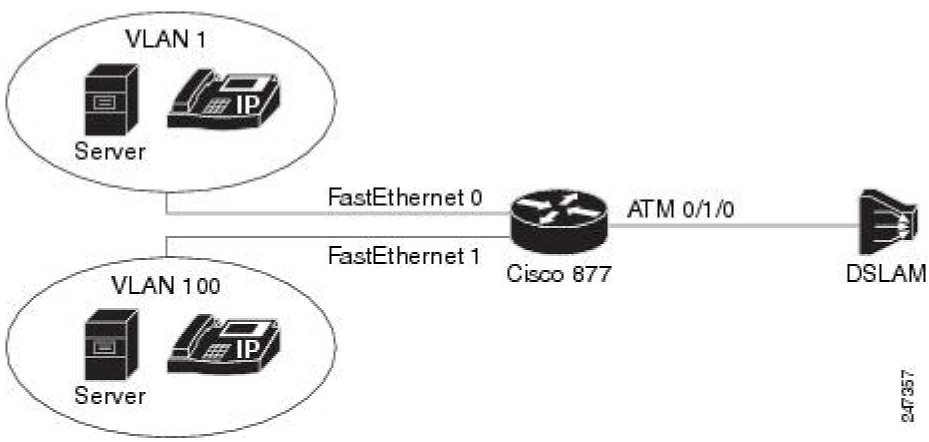
VLAN-Based Service Differentiation over ADSL

VLAN-based service differentiation allows service providers to offer a range of broadband-enabled services and applications to end users. It supports IP connectivity applications that require real-time network performance and applications that use best-effort, or Internet-grade performance.

The original VLAN tag in an inbound packet is changed to the value configured by the **bridge-dot1q encap** command before the tag leaves the device. For example, if you enter the command **bridge-dot1q encap 10**, a VLAN tag of 70 in a packet inbound from the local network is changed to a value of 10 in the egress packet. Any 802.1P value is changed to 0, and frames without VLAN tags are sent out over ATM with an added VLAN header as shown in the figure in the “Transporting 802.1P Marked 802.1Q Tags” section.

From an Ethernet perspective, this service is carried over a dedicated VLAN from the hand-over point to the end-user premises. This VLAN-based service differentiation at the PVC level is shown in the figure below.

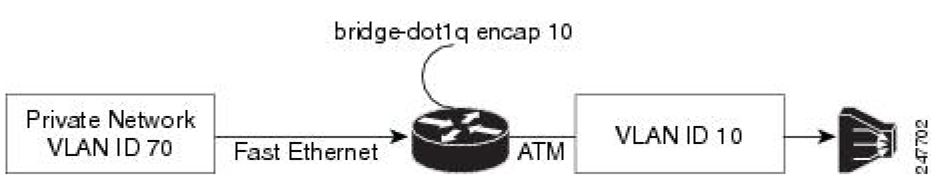
Figure 46: VLAN-Based Service Differentiation at PVC Level



The Ethernet VLAN used by the voice, video, and data services must be identified at the customer premises by an 802.1Q VLAN ID configured using the **bridge-dot1q encap** command. The VLAN is identified at the service provider’s end by a service-provider-assigned 802.1ad customer VLAN ID.

The **bridge-dot1q encap** command changes the local VLAN ID to the VLAN ID required by the service provider. The operation of this command is shown in the figure below.

Figure 47: Operation of the bridge-dot1q encap Command



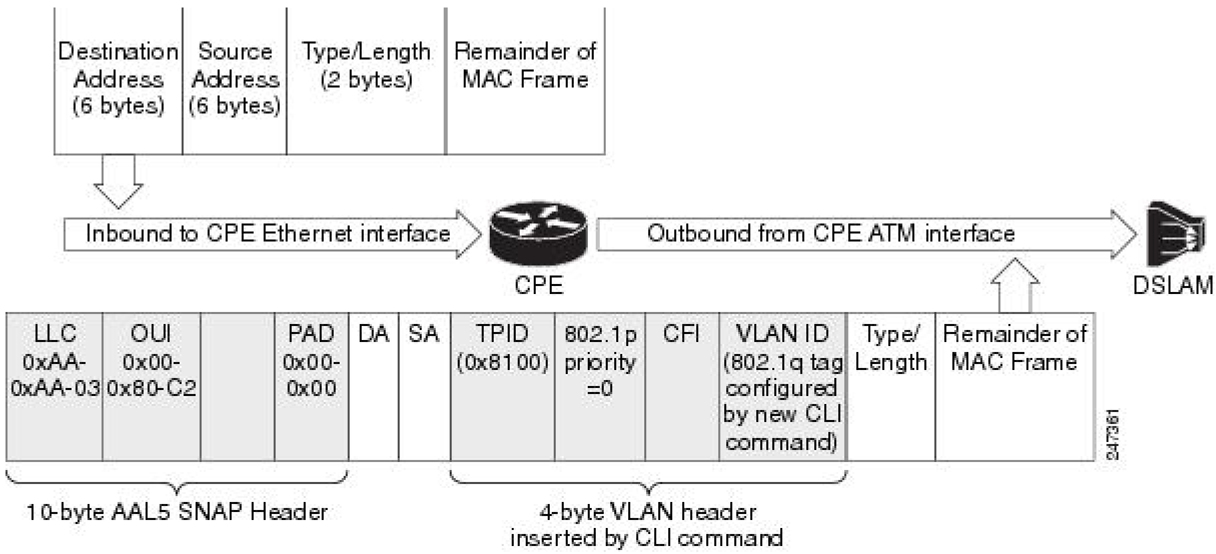
The figures in the “Transporting 802.1P Marked 802.1Q Tags” section show the PDU data structure in greater detail.

Transporting 802.1P Marked 802.1Q Tags

An 802.1Q VLAN tag is inserted into the MAC Protocol Data Unit (PDU), and this PDU is sent to the Digital Subscriber Line Access Multiplexer (DSLAM). Incoming and outgoing PDU structures are shown in the two figures below.

The figure below shows the packet structure when the incoming Ethernet frames do not have a VLAN header.

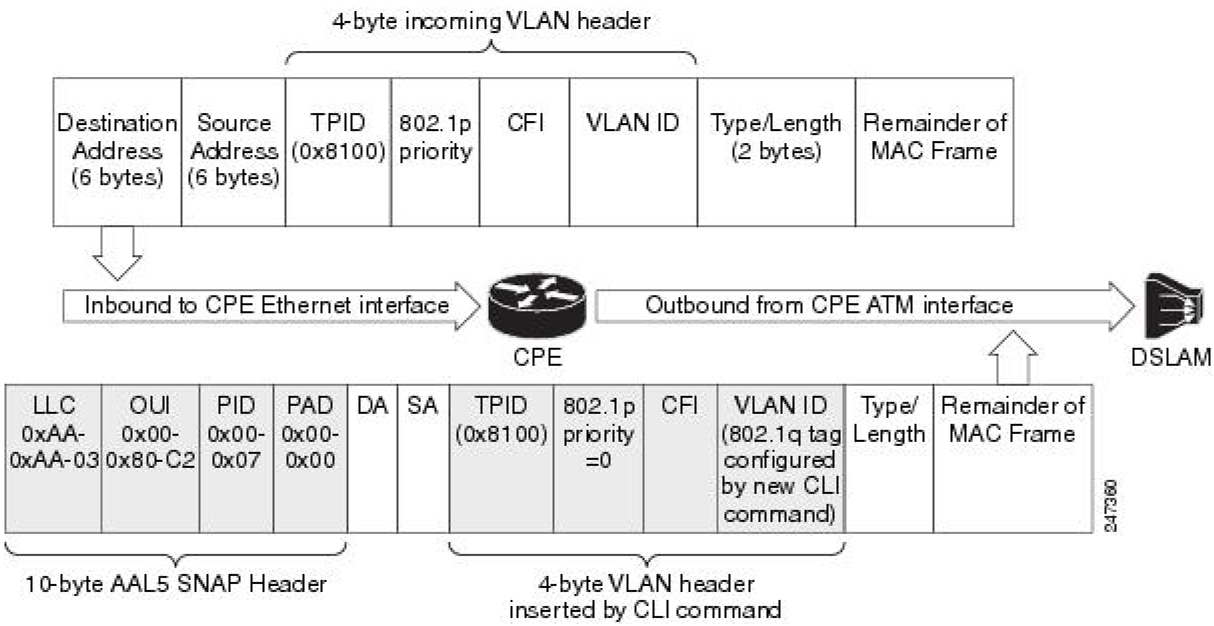
Figure 48: Incoming and Outgoing Packet Structures When No Incoming VLAN ID Is Present



The figure below shows that a 4-byte VLAN header has been inserted in the outgoing packet, with an 802.1P value. The VLAN ID value is configured by the **bridge-dot1q encap** command.

The figure below shows the incoming packet structure when the incoming Ethernet packets contain a VLAN header.

Figure 49: Incoming and Outgoing Packet Structures When an Incoming VLAN ID Is Present



The outgoing packet structure is the same as in figure 1.

Note The 802.1P priority that was configured earlier is changed to 0, and any VLAN ID that is configured is set to the ID configured by the **bridge-dot1q encap** command.

The CPE is connected to the DSLAM via an ATM interface that is configured as the bridging interface. The CPE establishes a PPP over Ethernet (PPPoE) session over the bridging ATM interface with the service provider. The VLAN and voice traffic enter customer devices via VLAN ports or a Switched Virtual Interface (SVI).

In the CPE, the packet is classified as data or voice traffic based on the VLAN ID, Differentiated Services Code Point (DSCP), protocol, source MAC address, or port. The packets are marked with the quality of service (QoS) group, and routed from VLAN via the Bridge Virtual Interface (BVI) to the ATM PVC bridging interface.

If the packet requires encapsulation, ATM provides the default VLAN ID. If there is a QoS service policy attached to the PVC, packets are classified against the QoS group. QoS marks the corresponding VLAN ID and 802.1P or class of service (CoS) value into the packet VLAN header. The QoS VLAN ID overwrites the default VLAN ID. If there is no service policy attached in PVC, the packets are sent out with the default VLAN ID and default CoS marking.

Packets returning from the service provider's network and destined to the customer's network carry VLAN tags. The ATM PVC interface removes the VLAN tag before passing it for further processing. These packets do not require classification or QoS marking.

Using PPPoE, the CPE device acts as a PPPoE Dialer client and gets the IP address dynamically from the service provider by using the Point-to-Point Protocol. The Dialer interface has to be configured and associated with the ATM PVC interface. The packets are sent out with the default VLAN ID as PPPoE supports only one VLAN ID per PVC. PPP control packets such as PPPoE Active Discovery Initiation (PADI), PPPoE Active Discovery Request (PADR), PPPoE Active Discovery Terminate (PADT) and keepalive packets are marked with higher priority CoS markings similar to the real-time traffic. The VLAN header has to be removed from the packet at the ingress interface (ATM PVC) when the packet returns.

How to Configure Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Configuring Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs

Perform this task to configure the Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature.

Note Only one **bridge-dot1q encap** *vlan-id* command can be configured under a PVC. Only one VLAN ID is allowed per session using PPPoE. The PPPoE session can be disconnected if the configured VLAN ID (set using the **set vlan-inner** or **bridge-dot1q encap** *vlanid* command) differs from the default VLAN ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map match-all egress**
4. **match qos-group** *number*
5. **class-map match-all ingress**
6. **match input-interface** *name*
7. **policy-map egress-policy**
8. **class egress**
9. **set cos-inner** *number*
10. **set vlan-inner** *number*
11. **exit**
12. **exit**
13. **policy-map ingress-policy**
14. **class ingress**
15. **set qos-group** *number*
16. **exit**
17. **exit**
18. Enter one of the following:
    - **interface atm** *interface-id* **point-to-point**
    - **interface atm** *slot* **/ 0 point-to-point**
    - **interface atm** *slot/ port-adaptor*/**0 point-to-point**
19. **bridge-group** *group-number*
20. **pvc** *vpi/vci*
21. **bridge-dot1q encap** *provider-vlan-id*
22. **encapsulation aal5snap**
23. **service-policy out egress-policy**
24. **pppoe-client dial-pool-number** *number*
25. **pppoe-client control-packets vlan cos** *number*
26. **service-policy input ingress-policy**
27. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map match-all egress** **Example:** `Device(config)# class-map match-all egress`	Determines how packets are evaluated when multiple match criteria exist for the egress.
Step 4	**match qos-group** *number* **Example:** `Device(config)# match qos-group 101`	Identifies a specific quality of service (QoS) group value as a match criterion. The range is from 0 to 1023.
Step 5	**class-map match-all ingress** **Example:** `Device(config)# class-map match-all ingress`	Determines how packets are evaluated when multiple match criteria exist for the ingress.
Step 6	**match input-interface** *name* **Example:** `Device(config)# match input-interface Vlan2`	Configures a class map to use the specified input interface as a match criterion.
Step 7	**policy-map egress-policy** **Example:** `Device(config)# policy-map egress-policy`	Creates or modifies a policy map that can be attached to one or more interfaces to specify an egress service policy and enters policy-map configuration mode.
Step 8	**class egress** **Example:** `Device(config-pmap)# class egress`	Specifies the name of the egress class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. Enters policy-map class configuration mode.
Step 9	**set cos-inner** *number* **Example:** `Device(config-pmap-c)# set cos-inner 5`	Sets the inner CoS value. The range is from 0 to 7.
Step 10	**set vlan-inner** *number* **Example:** `Device(config-pmap-c)# set vlan-inner 333`	(For PPPoE) Sets the inner VLAN value. The range is from 1 to 4094.
Step 11	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.

	Command or Action	Purpose
Step 12	**exit** **Example:** `Device(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.
Step 13	**policy-map ingress-policy** **Example:** `Device(config)# policy-map ingress-policy`	Creates or modifies a policy map that can be attached to one or more interfaces to specify an ingress service policy and enters policy-map configuration mode.
Step 14	**class ingress** **Example:** `Device(config-pmap)# class ingress`	Specifies the name of the ingress class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy. Enters policy-map class configuration mode
Step 15	**set qos-group** *number* **Example:** `Device(config-pmap-c)# set qos-group 101`	Sets the CoS value for a CoS group. The range is from 0 to 1023.
Step 16	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 17	**exit** **Example:** `Device(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.

Step 18	Enter one of the following:
	• **interface atm** *interface-id* **point-to-point**
	• **interface atm** *slot* **/ 0 point-to-point**
	• **interface atm** *slot/ port-adaptor*/**0 point-to-point**
	
	Example:
	`Device(config)# interface atm0 point-to-point`
	
	Example:
	`Device(config)# interface atm 0/0 point-to-point`
	
	Example:
	`Device(config)# interface atm 0/1/0.1 point-to-point`
		Specifies the ATM point-to-point interface using the appropriate format of the command and enters interface or subinterface configuration mode.

	Command or Action	Purpose
Step 19	**bridge-group** *group-number* **Example:** `Device(config-if)# bridge-group 1`	Assigns the interface or subinterface to a bridge group.
Step 20	**pvc** *vpi/vci* **Example:** `Device(config-if)# pvc 9/117`	Creates a PVC of a specified virtual path identifier (VPI)/virtual circuit identifier (VCI) number and enters interface ATM VC configuration mode or subinterface ATM VC configuration mode.
Step 21	**bridge-dot1q encap** *provider-vlan-id* **Example:** `device(config-if-atm-vc)# bridge-dot1q encap`	Enables the router to include the 802.1Q VLAN ID in the MAC PDU. The service provider VLAN ID range is from 1 to 4094.
Step 22	**encapsulation aal5snap** **Example:** `Device(config-if-atm-vc)# encapsulation aal5snap`	Specifies the ATM Adaptation Layer 5 (AAL5) encapsulation type. AAL5SNAP is used so that two or more protocols can be multiplexed over the virtual circuit.
Step 23	**service-policy out egress-policy** **Example:** `Device(config-if-atm-vc)# service-policy out egress-policy`	Defines the service policy at the egress.
Step 24	**pppoe-client dial-pool-number** *number* **Example:** `Device(config-if-atm-vc)# pppoe-client dial-pool-number 1`	Configures a PPP over Ethernet (PPPoE) client and specifies dial-on-demand routing (DDR) functionality.
Step 25	**pppoe-client control-packets vlan cos** *number* **Example:** `Device(config-if-atm-vc)# pppoe-client control-packets vlan cos 6`	Enables CoS marking for PPPoE control packets on the PPPoE client.
Step 26	**service-policy input ingress-policy** **Example:** `Device(config-if-atm-vc)# service-policy input ingress-policy`	Defines the service policy at the ingress.
Step 27	**end** **Example:** `Device(config-if-atm-vc)#` **end**	Exits interface ATM VC configuration mode, or subinterface ATM VC configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

To troubleshoot PPP sessions establishment, use the following commands:

- **debug ppp authentication**
- **debug ppp negotiation**

To troubleshoot the establishment of PPP sessions that are authenticated by a RADIUS or TACACS server, use the following commands:

- **debug aaa authentication**
- **debug aaa authorization**

Caution Use **debug** commands with extreme caution because they are CPU-intensive and can seriously impact your network.

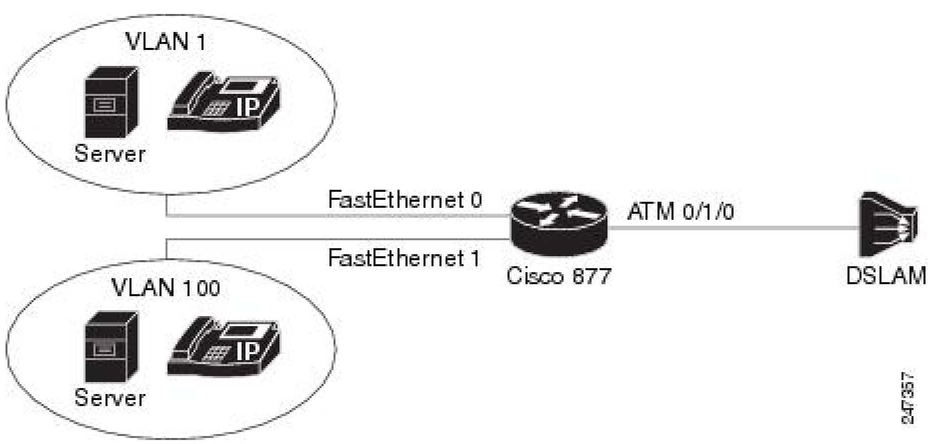
Configuration Examples for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Example: Traffic from Multiple Incoming VLANs Bridged to a VLAN

The following example shows how the traffic from multiple incoming VLANs is bridged to a single outgoing VLAN. The traffic arrives on Layer 2 Fast Ethernet ports and a DHCP server assigns IP addresses on the private network. Network Address Translation (NAT) is enabled. A static IP address is used on the outgoing Bridge-Group Virtual Interface (BVI) interface.

This topology is shown in the figure below.

Figure 50: Topology: Traffic from Multiple Incoming VLANs Bridged to a Single Outgoing VLAN



The following configuration is for the Cisco 877 router.

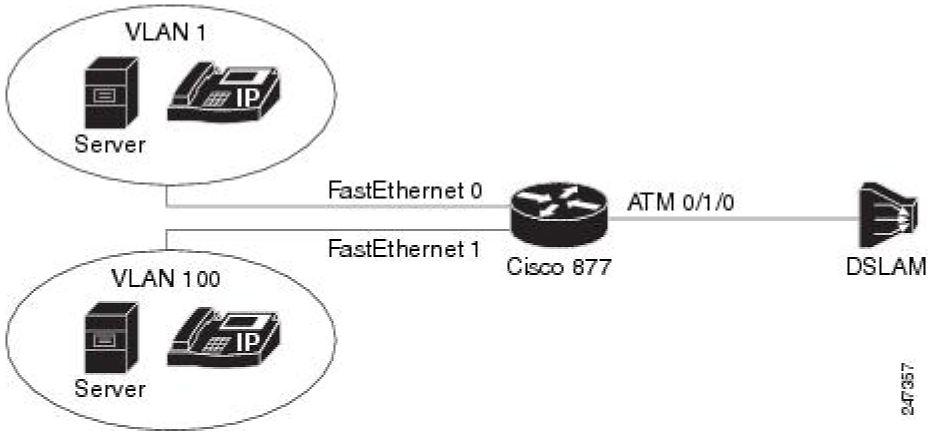
```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool test_pool1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool test_pool2
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
!
!
bridge irb
!
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 bridge-group 1
 bridge-group 1 spanning-disabled
 pvc 0/110
  bridge-dot1q encap 10
  encapsulation aal5snap
!
interface FastEthernet0
 switchport access vlan 1
!
interface FastEthernet1
 switchport access vlan 100
!
interface Vlan1
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Vlan100
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface BVI1
 ip address 10.0.0.0 255.0.0.0
 ip nat outside
 ip virtual-reassembly
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip nat pool test 10.0.0.0 10.0.0.0 netmask 255.0.0.0
ip nat inside source list 101 pool test overload
ip nat inside source list 102 pool test overload
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 any log
access-list 102 permit ip 192.168.20.0 0.0.0.255 any log
!
bridge 1 protocol ieee
bridge 1 route ip
!
```

Example: Traffic from Multiple VLANs Arrives at the Router over a Layer 3 Port

The following example shows how traffic from multiple VLANs arrives at the router over a Layer 3 port. All this traffic is bridged over a single ATM virtual circuit to the service provider’s DSLAM and tagged with a single VLAN tag. Both WAN and LAN IP addresses are provided by DHCP servers.

This topology is shown in the figure below.

Figure 51: Topology: Traffic From Multiple VLANs Arrives at the Router over a Layer 3 Port



The following configuration is for the Cisco 877 router.

```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool test_pool1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool test_pool2
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
!
bridge irb
!
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
 interface FastEthernet0/1.1
 encapsulation dot1Q 100
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet0/1.2
 encapsulation dot1Q 1 native
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface ATM0/1/0
 no ip address
 no atm ilmi-keepalive
!
!
interface ATM0/1/0.1 point-to-point
 bridge-group 1
 bridge-group 1 spanning-disabled
 pvc 9/117
  bridge-dot1q encap 10
  encapsulation aal5snap
!
```

```
!
interface BVI1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
!
ip forward-protocol nd
!
ip nat inside source list 101 interface BVI1 overload
ip nat inside source list 102 interface BVI1 overload
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 any log
access-list 102 permit ip 192.168.20.0 0.0.0.255 any log
!
bridge 1 protocol ieee
bridge 1 route ip
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List , All Releases
ATM commands	Cisco IOS Asynchronous Transfer Mode Command Reference

Standards and RFCs

Standard/RFC	Title
IEEE 802.1P	*Traffic Class Expediting and Dynamic Multicast Filtering*
IEEE 802.1Q	*Virtual LANs*
IEEE 802.3	*LAN/MAN CSMA/CD (Ethernet) Access Method*
ITU-T G.992.1 (G.dmt)	*Asymmetrical Digital Subscriber Line (ADSL) Transceivers*
ITU-T G.992.5	*Asymmetrical Digital Subscriber Line (ADSL) Transceivers-Extended Bandwidth ADSL2 (ADSL2+)*
ITU-T I363.5	*B-ISDN ATM Adaptation Layer Specification: Type 5 AAL*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 33: Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Feature Name	Releases	Feature Information
Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks	15.1(2)T	The Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature allows 802.1P marking based on 802.1Q tags and transportation of these tags over ATM PVC used in ADSL2+ uplinks. The following commands were introducef: **pppoe-client control-packets vlan cos**, **set vlan-inner**.
Transporting VLAN Tags over DSL Links	15.0(1)XA	The Transporting VLAN Tags over DSL Links feature allows 802.1Q tags to be transported over ATM PVCs used in ADSL2+ uplinks. The following command was introducef: **bridge-dot1q encap**.

Glossary

802.1ad—An amendment to IEEE 802.1Q that enables a service provider to offer bridged VLANs over its network.

802.1P—A 3-bit field within an Ethernet frame header added when using IEEE 802.1Q on an IEEE 802.1D network. It specifies a priority value from 0 and 7 that can be used by quality of service (QoS) disciplines to differentiate traffic.

802.1Q—A networking standard written by the IEEE 802.1 workgroup allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks. 802.1Q is commonly referred to as VLAN tagging.

AAL5SNAP—ATM Adaptation Layer 5 Subnetwork Protocol Access Protocol. A type of network encapsulation that supports multiplexing of two or more protocols over a virtual circuit.

ATM—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

BVI—Bridge Group Virtual Interface. A logical Layer 3-only interface associated with a bridge group when integrated bridging and routing (IRB) is configured.

CPE—Customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. This term can also refer to any telephone equipment residing on the customer site.

CVLAN—Customer Virtual Local Area Network.

DSL—Digital subscriber line. A public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL.

DSLAM—Digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

IRB—Integrated routing and bridging. Integrated Services Digital Network (ISDN) User Part. An upper-layer application supported by Signalling System 7 for connection setup and tear down.

NAT—Network Address Translation. A mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

PVC—Permanent virtual circuit (or connection). A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, this is called a permanent virtual connection.

VoIP—Voice over IP. The capability to carry normal telephony-style voice over an IP-based Internet with plain old telephone service (POTS) like functionality, reliability, and voice quality.

CHAPTER 27

Reuse MAC for ATM Route-Bridge Encapsulation

The Reuse MAC for ATM Route-Bridge Encapsulation feature provides for a configurable MAC address for ATM point-to-point sub-interfaces, with the single VC on each sub-interface that connects each subscriber to the ISP.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information for Define Interface Policy-Map AV Pairs AAA.

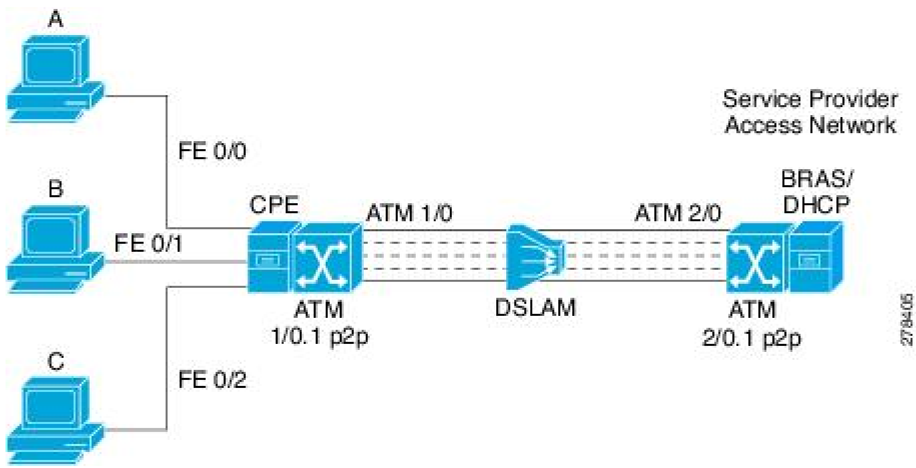
Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Reuse MAC for ATM Route-Bridge Encapsulation

When multiple hosts are connected to the Customer Premises Equipment (CPE) that in turn communicate to the Internet Service Provider (ISP) through the Broadband Remote Access Server (BRAS), the hosts are connected to the CPE through Ethernet and legacy ATM between the CPE and the BRAS, and aggregation using DSL Access Multiplexer (DSLAM).

In a standard setup, hosts are connected to the BRAS through sub-interfaces. A host sends a DHCP request to get its IP address from the DHCP server (can be the BRAS), and when the IP address is assigned, the packets start flowing with the IP. The ATM interface in the CPE is configured with Route-Bridge Encapsulation (RBE) to enable packets from the hosts to be bridged across the ATM connection as shown in the figure below.

Figure 52: Sample Topology for Reuse MAC for ATM Route-Bridge Encapsulation



The Reuse MAC for ATM Route-Bridge Encapsulation feature provides for a configurable MAC address for ATM point-to-point sub-interfaces, with the single virtual circuit (VC) on each sub-interface that connects each subscriber to the ISP.

How to Configure Reuse MAC for ATM Route-Bridge Encapsulation

The Reuse MAC for ATM Route-Bridge Encapsulation configuration is available only in the ATM point-to-point sub-interface mode. Only physical Ethernet interfaces can be used as client interfaces whose MAC address can be used for the ATM P2P sub-interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot/port*
4. **atm ether-mac-address** *interface-name*
5. **atm ether-mac-address** *mac-address*
6. **end**
7. **show running interface atm** *slot /port*

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	**interface atm** *slot/port* **Example:** `Router(config)# interface atm 1/0.1`	Specifies the ATM interface to be configured and enters ATM point-to-point sub-interface mode, where: • slot/port--Specifies the location of the interface
Step 4	**atm ether-mac-address** *interface-name* **Example:** `Router(config-subif)# atm ether-mac-address interface fastEthernet 0/0`	Specifies the interface name whose MAC address can be used to configure the ATM point-to-point sub-interfaces. This is option 1, skip step 5 if you prefer to specify the interface name and not the MAC address. **Note** Step 4 and step 5 are exclusive of each other.
Step 5	**atm ether-mac-address** *mac-address* **Example:** `Router(config-subif)# atm ether-mac-address 00a1.0b65.87bc`	Specifies the user defined or explicit MAC address that can be used to configure the ATM point-to-point sub-interfaces. This is option 2, skip step 4 if you prefer to specify the MAC address and not the interface name. **Note** Step 4 and step 5 are exclusive of each other.
Step 6	**end** **Example:** `Router(config-subif)# end`	Returns to the privileged EXEC mode.
Step 7	**show running interface atm** *slot /port* **Example:** `Router# show running interface atm0/0.000`	Displays the configuration.

Configuration Examples for Reuse MAC for ATM Route-Bridge Encapsulation

The following example shows how to configure the Reuse MAC for ATM Route-Bridge Encapsulation feature using an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface atm 3/0.100 point-to-point
Router(config-subif)# atm ether-mac-address interface fastEthernet 0/0
Router(config-subif)# end
```

The following example shows how to configure the Reuse MAC for ATM Route-Bridge Encapsulation feature using an MAC address for the ATM point-to-point sub-interface:

```
Router> enable
Router# configure terminal
Router(config)# interface atm 3/0.100 point-to-point
Router(config-subif)# atm ether-mac-address 00a1.0b65.87bc
```

Router(config-subif)# end

3. You can use the show run interface atm slot/port command to display the configuration:

```
Router# show run interface atm0/0.000
Current configuration : 188 bytes
!
interface ATM3/0.100 point-to-point
 atm route-bridged ip
 atm ether-mac-address interface FastEthernet0/0
 no atm enable-ilmi-trap
 pvc 1/100
 !
end
```

Additional References

The following sections provide references related to the ATM OAM Ping feature.

Related Documents

Related Topic	Document Title
Configuring PVCs and mapping a protocol address to a PVC while configuring ATM	Configuring PVCs section of *Cisco IOS Configuring ATM Feature Guide*
Configuring ATM	*Cisco IOS Configuring ATM Feature Guide*
ATM commands, complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Asynchronous Transfer Mode Command Reference*
Configuring ATM OAM traffic reduction	"ATM OAM Traffic Reduction" feature module

Related Topic	Document Title
Configuring PVCs with or without OAM	"Using OAM for PVC Management" sample configuration
Detecting failures when using OAM cells and PVC management	Troubleshooting PVC Failures When Using OAM Cells and PVC Management technical note
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
ITU-T Specification I.610 (ITU-T specification for B-ISDN operation and maintenance principles and functions).	I.610 Series I: Integrated Services Digital Network Maintenance principles

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Reuse MAC for ATM Route-Bridge Encapsulation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 34: Feature Information for Reuse MAC for ATM Route-Bridge Encapsulation

Feature Name	Releases	Feature Information
Reuse MAC for ATM Route-Bridge Encapsulation	15.1(1)T	The Reuse MAC for ATM Route-Bridge Encapsulation feature provides for a configurable MAC address for ATM point-to-point sub-interfaces, with the single VC on each sub-interface that connects each subscriber to the ISP. This feature was introduced in Cisco IOS RElease 15.1(1)T. The following commands were introducef: **atm ether-mac-address**.

INDEX

A

B

C

D

E

F

H

I

K

L

T

U

V

W