LAN ATM

About Cisco IOS Software Documentation

Last Updated: November 20, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section contains the following topics:

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS software uses the following program code conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

Cisco IOS documentation uses the following conventions for reader alerts:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

Cisco IOS Documentation Set

The Cisco IOS documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the organization of the Cisco IOS documentation set and how to access various document types.

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.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized by technology. 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.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references contain commands for Cisco IOS software for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

http://www.cisco.com/go/techdocs

Table 1 Cisco IOS Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS AppleTalk Configuration Guide* • *Cisco IOS AppleTalk Command Reference*	AppleTalk protocol.
• *Cisco IOS Asynchronous Transfer Mode Configuration Guide* • *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging Command Reference* • *Cisco IOS IBM Networking Command Reference*	Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
• *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).
• *Cisco IOS Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	Operations, Administration, and Maintenance (OAM); Ethernet connectivity fault management (CFM); ITU-T Y.1731 fault management functions; Ethernet Local Management Interface (ELMI); MAC address support on service instances, bridge domains, and pseudowire; IEEE 802.3ad Link Bundling; Link Aggregation Control Protocol (LACP) support for Ethernet and Gigabit Ethernet links and EtherChannel bundles; LACP support for stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles; and Link Layer Discovery Protocol (LLDP) and media endpoint discovery (MED).
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
• *Cisco IOS DECnet Configuration Guide* • *Cisco IOS DECnet Command Reference*	DECnet protocol.
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS Flexible NetFlow Configuration Guide* • *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS High Availability Configuration Guide* • *Cisco IOS High Availability Command Reference*	A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
• *Cisco IOS Integrated Session Border Controller Command Reference*	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
• *Cisco IOS Intelligent Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
• *Cisco IOS Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
• *Cisco IOS IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
• *Cisco IOS IP Application Services Configuration Guide* • *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
• *Cisco IOS IP Mobility Configuration Guide* • *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
• *Cisco IOS IP Multicast Configuration Guide* • *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
• *Cisco IOS IP Routing: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).
• *Cisco IOS IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
• *Cisco IOS IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	Routing Information Protocol (RIP).
• *Cisco IOS IP SLAs Configuration Guide* • *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
• *Cisco IOS IP Switching Configuration Guide* • *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
• *Cisco IOS IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document.
• *Cisco IOS ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).
• *Cisco IOS LAN Switching Configuration Guide* • *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
• *Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide* • *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
• *Cisco IOS Mobile Wireless Home Agent Configuration Guide* • *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
• *Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide* • *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
• *Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide* • *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Multiprotocol Label Switching Configuration Guide* • *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.
• *Cisco IOS Multi-Topology Routing Configuration Guide* • *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
• *Cisco IOS NetFlow Configuration Guide* • *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, and export features.
• *Cisco IOS Network Management Configuration Guide* • *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).
• *Cisco IOS Novell IPX Configuration Guide* • *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
• *Cisco IOS Optimized Edge Routing Configuration Guide* • *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
• *Cisco IOS Security Command Reference*	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters.
• *Cisco IOS Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS Security Configuration Guide: Securing the Control Plane*	Control Plane Policing, Neighborhood Router Authentication.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Security Configuration Guide: Securing User Services*	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
• *Cisco IOS Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.
• *Cisco IOS Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *Cisco IOS Service Selection Gateway Configuration Guide* • *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
• *Cisco IOS Software Activation Configuration Guide* • *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
• *Cisco IOS Software Modularity Installation and Configuration Guide* • *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
• *Cisco IOS Virtual Switch Command Reference*	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). **Note** For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
• *Cisco IOS VPDN Configuration Guide* • *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
• *Cisco IOS Wireless LAN Configuration Guide* • *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS System Message Guide	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator.
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is released monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Cisco IOS Asynchronous Transfer Mode Configuration Guide, Release 12.2(33)SR

Release 12.2(33)SR
November 20, 2009

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

Text Part Number:

Cisco IOS Asynchronous Transfer Mode Configuration Guide, Release 12.2(33)SR

Using the Command-Line Interface in Cisco IOS Software

Last Updated: October 14, 2009

This document provides basic information about the command-line interface (CLI) in Cisco IOS software and how you can use some of the CLI features. This document contains the following sections:

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS Software Documentation" document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product/Technologies Support area of Cisco.com at http://www.cisco.com/go/techdocs.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on Cisco ASR 1000 series routers)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes the purpose of the CLI interactive Help commands.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the Help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'. If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

```
Router(config)# we<Tab> webvpn
```

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>

Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>

Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a numeral. Spaces are also valid password characters; for example, "two words" is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

  Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples are from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

Caution Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

The following three output modifiers are available:

- **begin** *regular-expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular-expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular-expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression "protocol."

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at "^" marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following document:

- *Cisco IOS Release 12.4T System Message Guide*

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved.

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
- Cisco Product/Technology Support

  http://www.cisco.com/go/techdocs
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl

---

Configuring ATM

First Published: November 27, 2007
Last Updated: January 28, 2009

This chapter describes how to configure ATM on the Cisco 2600 series, Cisco 3600 series, Cisco 4500, Cisco 4700, Cisco 7100, Cisco 7200 series, Cisco 7500 and Cisco 12000 series routers. For further general information about ATM, see the chapter "Wide-Area Networking Overview" at the beginning of this book.

For a complete description of the ATM commands in this chapter, refer to the chapter "ATM Commands" in the *Cisco IOS Wide-Area Networking Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the section "Identifying Supported Platforms" in the chapter "Using Cisco IOS Software."

For information on the following related topics, see the corresponding Cisco publications:

Task	Resource
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 later 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*
Configuring PPP over ATM	"Configuring PPP over ATM" section in the "Configuring Broadband Access: PPP and Routed Bridge Encapsulation" chapter in this book

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Task	Resource
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

Note Beginning in Cisco IOS Release 11.3, all commands supported on the Cisco 7500 series routers are also supported on Cisco 7000 series routers equipped with RSP7000.

ATM Configuration Task List

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 the ATM Interface (Required)
- Configuring PVCs (Required)
- Configuring SVCs (Required)
- Configuring VC Classes (Optional)
- Configuring VC Management (Optional)
- Configuring Classical IP and ARP over ATM (Optional)
- Customizing the ATM Interface (Optional)
- Configuring ATM Subinterfaces for SMDS Networks (Optional)
- Configuring Fast-Switched Transparent Bridging for SNAP PVCs (Optional)
- Configuring Inverse Multiplexing over ATM (Optional)
- Configuring ATM E.164 Auto Conversion (Optional)
- Configuring Circuit Emulation Services (Optional)
- Configuring ATM Access over a Serial Interface (Optional)
- Troubleshooting the ATM Interface (Optional)
- Monitoring and Maintaining the ATM Interface (Optional)

See the section "ATM Configuration Examples" at the end of this chapter for configuration examples.

Enabling the ATM Interface

This section describes how to configure an ATM interface. For the 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.

To configure the ATM interface, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode from the terminal.
Step 2	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `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	`Router(config-if)# 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.

To enable the ATM interface, use the following command in interface configuration mode:

Command	Purpose
`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.

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" for more information.

All virtual circuit characteristics listed in the chapter "Wide-Area Networking Overview" apply to these PVCs. 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 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 (Required)
- Mapping a Protocol Address to a PVC (Required)

- Configuring the AAL and Encapsulation Type (Optional)
- Configuring PVC Traffic Parameters (Optional)
- Configuring PVC Discovery (Optional)
- Enabling Inverse ARP (Optional)
- Configuring Generation of End-to-End F5 OAM Loopback Cells to Verify Connectivity (Optional)
- Configuring Broadcast on a PVC (Optional)
- Assigning a VC Class to a PVC (Optional)
- Configuring PVC Trap Support (Optional)

Creating a PVC

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.

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.

Once you specify a name for a PVC, you can reenter the interface-ATM-VC configuration mode by simply entering **pvc** *name*.

Note 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" 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.

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.

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" at the end of this chapter.

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 Wide-Area Networking 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.

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.)

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 "Configuring an ABR PVC Example" 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."

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.

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. 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.

For an example of configuring an ABR PVC, see the section "Configuring an ABR PVC Example" later in this chapter.

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).

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
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.

	Command	Purpose
Step 6	`Router(config)# interface atm slot/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm slot/port-adapter/0[.subinterface-number {multipoint | point-to-point}]` or `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.
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.

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 "Configuring PVC Discovery Example" 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.

For an example of configuring PVC discovery, refer to the section "Configuring PVC Discovery Example" at the end of this chapter.

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.

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm slot/port-adapter/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm number[.subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
Step 2	`Router(config-if)# pvc [name] vpi/vci`	Specifies an ATM PVC by name (optional) and VPI/VCI numbers.
Step 3	`Router(config-if-atm-vc)# encapsulation aal5snap`	Configures AAL5 LLC-SNAP encapsulation if it is not already configured.
Step 4	`Router(config-if-atm-vc)# inarp minutes`	(Optional) Adjusts the Inverse ARP time period.

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

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 Wide-Area Networking Command Reference*.

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

Configuring Generation of End-to-End F5 OAM 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.

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

	Command	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.

For information about managing PVCs using OAM, see the section "Configuring OAM Management" later in this chapter.

For an example of OAM loopback cell generation, see the section "Configuring Generation of End-to-End F5 OAM Loopback Cells Example" at the end of this chapter.

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:

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

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" 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" 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), not 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" 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. To enable PVC trap support and OAM management, use the following commands beginning in global configuration mode:

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

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

For more information on OAM management, see the section "Configuring OAM Management" 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 "Configuring PVC Trap Support Example" at the end of this chapter.

Configuring SVCs

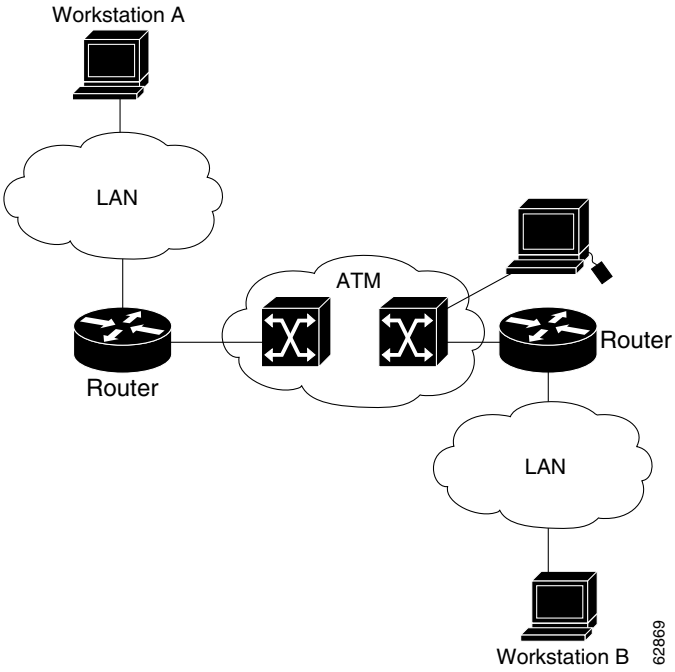
ATM switched virtual circuit (SVC) service operates much like X.25 SVC service, although ATM allows much higher throughput. Virtual circuits are created and released dynamically, providing user bandwidth on demand. This service requires a signalling protocol between the router and the switch.

The ATM signalling software provides a method of dynamically establishing, maintaining, and clearing ATM connections at the User-Network Interface (UNI). The ATM signalling 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.

Figure 1 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



To use SVCs, complete the tasks in the following sections:

- Configuring Communication with the ILMI (Required)
- Configuring the PVC That Performs SVC Call Setup (Required)
- Configuring the NSAP Address (Required)
- Creating an SVC (Required)

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 should not have to perform these tasks unless you need to customize your particular SVC connection.

- Configuring ATM UNI Version Override (Optional)
- Configuring the Idle Timeout Interval (Optional)
- Configuring Point-to-Multipoint Signalling (Optional)
- Configuring IP Multicast over ATM Point-to-Multipoint Virtual Circuits (Optional)
- Configuring SVC Traffic Parameters (Optional)
- Configuring Strict Traffic Shaping (Optional)
- Configuring Generation of End-to-End F5 OAM Loopback Cells to Verify Connectivity (Optional)
- Configuring Broadcast on an SVC (Optional)
- Assigning a VC Class to an SVC (Optional)

- Configuring SSCOP (Optional)
- Closing an SVC (Optional)

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 the router can receive SNMP traps and new network prefixes. The recommended *vpi* and *vci* values for the ILMI PVC are 0 and 16, respectively. To configure ILMI communication, 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.

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

Once you have configured an ILMI PVC, you can optionally enable the ILMI keepalive function by using the following command in interface configuration mode:

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

No other configuration steps are required.

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 "Configuring Communication with the ILMI Example" in the "ATM Configuration Examples" section at the end of this chapter.

Configuring the PVC That Performs SVC Call Setup

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

For out-of-band signalling, a signalling PVC must be configured before any SVCs can be set up. Figure 2 illustrates that a signalling 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 Signalling PVC

To configure the signalling 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 signalling PVC for an ATM main interface that uses SVCs.

Note This signalling 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 "SVCs in a Fully Meshed Network Example" at the end of this chapter for a sample ATM signalling configuration.

Configuring the NSAP Address

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

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

- Configuring the ESI and Selector Fields
- Configuring the Complete NSAP Address

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.

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:

	Command	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.

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" 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 "SVCs with Multipoint Signalling Example" at the end of this chapter.

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.

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.

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."

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

Creating an SVC

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

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

	Command	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 aal5encap`	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type.
Step 3	`Router(config-if-atm-vc)# protocol protocol protocol-address [[no] broadcast]`	Maps a protocol address to 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.

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

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.

No other configuration steps are required.

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.

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.

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

Configuring Point-to-Multipoint Signalling

Point-to-multipoint signalling (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 signalling on an ATM interface after you have mapped protocol addresses to NSAPs and configured one or more protocols for broadcasting.

After multipoint signalling 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.

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
Step 2	`Router(config-if)# pvc [name] 0/5 qsaal`	Configures the signalling 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` and `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.

	Command	Purpose
Step 5	`Router(config-if)# atm nsap-address nsap-address` or `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 signalling to the ATM switch.
Step 10	`Router(config-if)# atm multipoint-interval interval`	(Optional) Limits the frequency of sending AddParty messages.

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

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 signalling.

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

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 signalling 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 Non Real-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.

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm slot/port-adapter/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm number[.subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
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	`Router(config-if-atm-vc)# ubr output-pcr [input-pcr]` or `Router(config-if-atm-vc)# ubr+ output-pcr output-mcr [input-pcr] [input-mcr]` or `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.

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

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 "Configuring SVC Traffic Parameters Example" 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."

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.

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.

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.

Configuring Generation of End-to-End F5 OAM Loopback Cells to Verify 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" section later in this chapter.

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

	Command	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.

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

Configuring Broadcast on an SVC

To send duplicate broadcast packets or send a single broadcast packet using multipoint signalling 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.

Note 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" 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" 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, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# sscop cc-timer seconds`	Sets the connection control timer.

To change the retry count of the connection control timer from the default value of 10, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# sscop max-cc retries`	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. To change the transmitter's window from the default value of 7, use the following command in interface configuration mode:

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

A receiver window controls how many packets can be received before an acknowledgment is required. To change the receiver's window from the default value of 7, use the following command in interface configuration mode:

Command	Purpose
`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 signalling 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" section later in this chapter for examples of VC class configurations.

To create and use a VC class, complete the tasks in the following sections:

- Creating a VC Class
- Configuring VC Parameters
- Applying a VC Class

Creating a VC Class

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

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

For examples of creating VC classes, see the section "Creating a VC Class Examples" at the end of this chapter.

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" and "Configuring PVC Trap Support" 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 "Creating a VC Class Examples" at the end of this chapter.

Applying a VC Class

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:

	Command	Purpose
Step 1	`Router(config-if)# pvc [name] vpi/vci` or `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.

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

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

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

For examples of applying a VC class to an ATM interface, see the section "Applying a VC Class Examples" later in this chapter.

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
- Configuring OAM Management

Configuring ILMI Management

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm slot/port-adapter/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm number[.subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
Step 2	`Router(config-if)# pvc [name] 0/16 ilmi`	Configures a PVC for communication with the ILMI.
Step 3	`Router(config)# interface atm slot/0.subinterface-number multipoint` or `Router(config)# interface atm slot/port-adapter/0.subinterface-number multipoint` or `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.

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

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.

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 "ILMI Management on an ATM PVC Example" at the end of this chapter.

Configuring OAM Management

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
- Configuring OAM Management for SVCs

Configuring OAM Management for PVCs

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0[.subinterface-number {multipoint | point-to-point}]` or `Router(config)# interface atm slot/port-adapter/0[.subinterface-number {multipoint | point-to-point}]` or `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.[1]
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 re-establishing and removing a PVC connection.

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

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.

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 "OAM Management on an ATM SVC Example" at the end of this chapter.

Configuring OAM Management for SVCs

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

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

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

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

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.

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

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
- Configuring the Router as an ATM ARP Server

Configuring the Router as an ATM ARP Client

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
Step 2	`Router(config-if)# atm esi-address esi.selector`	Specifies the ATM address of the interface.
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 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.

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

You can designate the current router interface as the ATM ARP server in Step 4 by typing **self** in place of **nsap** *nsap-address*.

To configure the ESI and selector fields in Step 2, 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" earlier in this chapter.

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

Configuring the Router as an ATM ARP Server

Cisco's implementation of the ATM ARP server supports rendundant 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.

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

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
Step 2	`Router(config-if)# atm esi-address esi.selector`	Specifies the ATM address of the interface.
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.

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

To configure the ESI and selector fields in Step 2, 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" earlier in this chapter.

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

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.

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:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
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.

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

Repeat Step 3 for each PVC you want to create.

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.

For an example of configuring the ATM Inverse ARP mechanism, see the section "Configuring ATM Inverse ARP in a PVC Environment Example" at the end of this chapter.

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
- Configuring MTU Size
- Setting the SONET PLIM
- Setting Loopback Mode
- Setting the Exception Queue Length
- Configuring the Maximum Number of Channels

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" for more information.

See the section "Dynamic Rate Queue Examples" 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:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
Step 2	`Router(config-if)# atm rate-queue tolerance svc [pvc] tolerance-value [strict]`	Configures a rate queue tolerance.

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

The value for the *tolerance-value* argument is 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.

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.

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. 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.

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

Setting Loopback Mode

To loop all packets back to your ATM interface instead of the network, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# loopback`	Sets loopback mode.

To loop the incoming network packets back to the ATM network, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# loopback line`	Sets line loopback mode.

Setting the Exception Queue Length

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

Note This command is supported only on the AIP.

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.

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.

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

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.

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.

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

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.

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.

Note This command is supported only on the AIP.

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.

To set the number of receive buffers, use the following command in interface configuration mode:

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

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.

To set the number of transmit buffers, use the following command in interface configuration mode:

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

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

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 generate 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.

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.

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

	Command	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.

	Command	Purpose
Step 4	`Router(config-if)# atm vp-filter hexvalue`	Configures a virtual path filter for the affected ATM subinterface.
Step 5	`Router(config-if)# pvc [name] vpi/vci smds`	Creates an AAL3/4 PVC.

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

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*.

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 "PVC with AAL3/4 and SMDS Encapsulation Examples" at the end of this chapter.

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:

	Command	Purpose
Step 1	`Router(config-if)# atm mid-per-vc maximum`	Limits the number of message identifiers allowed per virtual circuit.
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 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.

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 for SNAP PVCs

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.

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

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

	Command	Purpose
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.

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

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 "Transparent Bridging on an AAL5-SNAP PVC Example" at the end of this chapter.

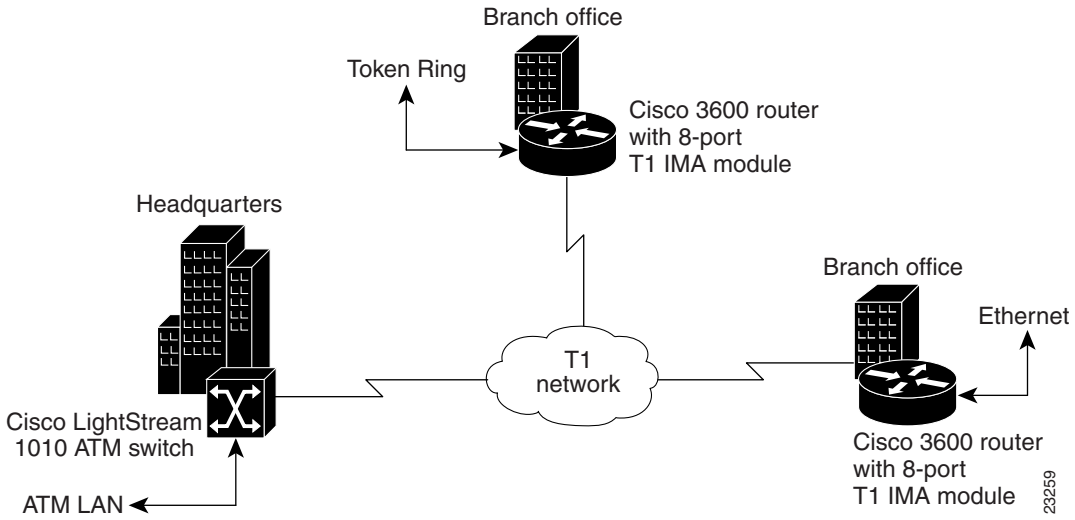
Configuring Inverse Multiplexing over ATM

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" 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. Figure 3 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



The following sections provide more specific information about IMA and how to configure it:

- IMA Protocol Overview
- General Description of ATM T1/E1 IMA
- IMA Configuration Task List
- Bandwidth Considerations
- Related Documents

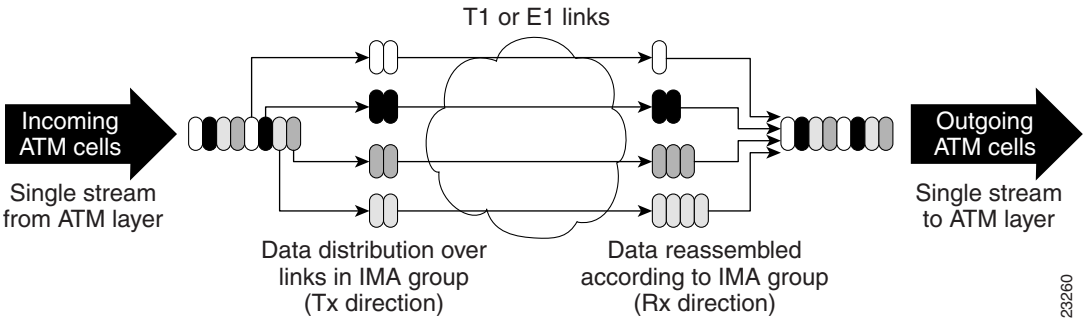
IMA Protocol Overview

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 out 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.

Figure 4 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 wtih 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 non-real-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.

- Configuring an ATM Interface for IMA Operation (Required)
- Verifying an ATM Interface Configured for IMA Operation (Optional)
- Configuring IMA Groups (Required)
- Verifying IMA Group Configuration (Optional)
- Troubleshooting Tips (Optional)

For examples of IMA configuration, see the section "Inverse Multiplexing over ATM Examples" 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 ATM Interface on the Multiport T1/E1 ATM Network Module for IMA Operation
- Configuring the ATM Interface on the Multiport T1/E1 ATM Port Adapter for IMA Operation

Configuring the ATM Interface on 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:

	Command	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	`Router(config-if)# cablelength long {gain26 | gain36} {-15db | -22.5db | -7.5db | 0db}` or `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 non-variable 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.
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 ATM Interface on 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:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/port` (Cisco 7100 series and 7200 series routers) or `Router(config)# interface atm slot/port-adapter/port` (Cisco 7500 series)	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. **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.

	Command	Purpose
Step 3	`Router(config-if)# lbo long {gain26 | gain36} {-15db | -22.5db | -7.5db | 0db}`	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.
	or `lbo short {133 | 266 | 399 | 533 | 655}`	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.

	Command	Purpose
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	`Router(config-if)# loopback [diagnostic |[payload | line] | remote [iboc | esf [payload | line]]]` for T1 `Router(config-if)# loopback [diagnostic | local [payload | line]]` for E1	(For testing only) Loops all packets from the ATM interface back to the interface, as well as directs the packets to the network. The default **line** setting places the interface into external loopback mode at the 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`[1]	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.
Step 10	`Router(config-if)# no shutdown`	Ensures that the link is active at the IMA level.

1. 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.

Verifying an ATM Interface Configured for IMA Operation

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

- Verifying an ATM Interface on the Multiport T1/E1 ATM Network Module
- Verifying an ATM Interface on the Multiport T1/E1 ATM Port Adapter

Verifying an ATM Interface on the Multiport T1/E1 ATM Network Module

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

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.

```
router# show interface atm 0/1
ATM0/1 is up, line protocol is up
  Hardware is ATM T1
  Internet address is 21.1.1.2/8
  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.

```
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 an ATM Interface on the Multiport T1/E1 ATM Port Adapter

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

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.

```
Router# show interface atm 5/0
ATM5/0 is up, line protocol is up
  Hardware is IMA PA
  Internet address is 156.0.2.0/16
  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.

```
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
- Configuring IMA Groups on the Multiport T1/E1 ATM Port Adapter

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:

	Command	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.
Step 13	`Router(config-if)# ima test [link port] [pattern pattern-id]`	Starts the IMA link test procedure with the specified link and pattern.

For examples of configuring IMA groups on Multiport T1/E1 ATM Network Modules, see the sections "E1 IMA on Multiport T1/E1 ATM Network Module Example" and "T1 IMA on Multiport T1/E1 ATM Network Module Example" at the end of this chapter.

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:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/imagroup number` (Cisco 7100 series and 7200 series routers) or `Router(config)# interface atm slot/port-adapter/ima group number` (Cisco 7500 series routers)	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. 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* indicates the 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 signalling for setup and teardown of SVCs by specifying the Q.SAAL[1] 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[2] 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	Purpose
Step 9	`Router(config-if)# ima clock-mode {common [port] | independent}`[3]	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]`	(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.

1. Q Signalling ATM adaptation Layer.
2. Subnetwork Access Protocol.
3. 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.

For an example of configuring IMA groups on multiport T1/E1 ATM port adapters, see the section "T1 IMA on Multiport T1/E1 ATM Port Adapter Example" at the end of this chapter.

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

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.

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.

```
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:

```
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.

```
 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.

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.

```
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.

```
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 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" earlier in this chapter and the **encapsulation aal5** command in the *Cisco IOS Wide-Area Networking 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."

Tip Use the **ping** command when the network is functioning properly to see how the command works under normal conditions and so that you can 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. Table 1 and Table 2 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
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 signalling 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. Table 3 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

Table 3 ATM and E1.64 Address Formats

Address Type	Example
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.

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:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0` or `Router(config)# interface atm slot/port-adapter/0` or `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
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 signalling 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.
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.

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

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 "Configuring ATM E.164 Auto Conversion Example" at the end of this chapter.

Configuring Circuit Emulation Services

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

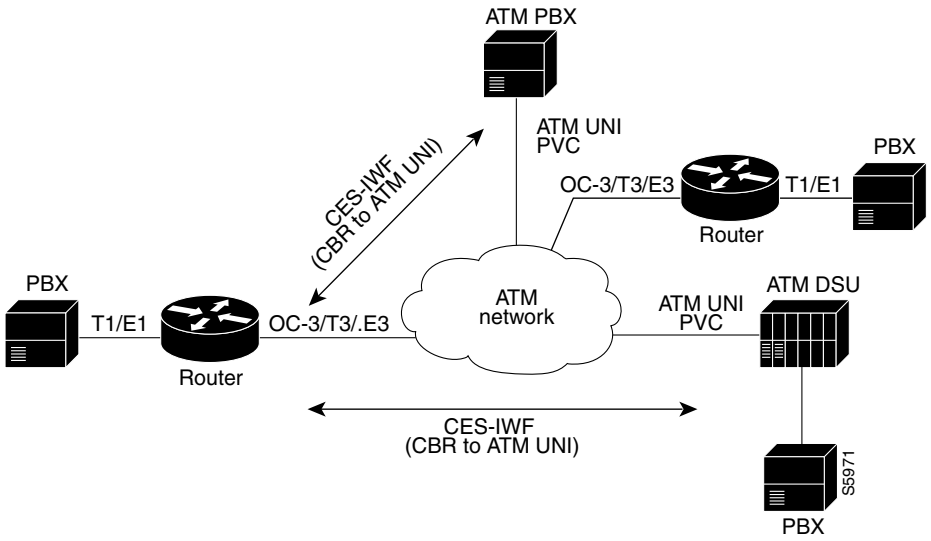
- CES Overview
- Configuring CES on the OC-3/STM-1 ATM Circuit Emulation Service Network Module
- Configuring CES on the ATM-CES Port Adapter
- Configuring Virtual Path Shaping

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.

Figure 5 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 OC-3/STM-1 ATM Circuit Emulation Service 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.

- OC-3/STM-1 ATM Circuit Emulation Service Network Module Restrictions
- Configuring the ATM Interface (Required)
- Configuring the T1/E1 Controller (Required)
- Activating the Connection (Required)
- Verifying CES Configuration on the OC-3/STM-1 ATM Circuit Emulation Service Network Module (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 "Configuring CES on an OC-3/STM-1 ATM Circuit Emulation Services Network Module Example" at the end of this chapter.

OC-3/STM-1 ATM Circuit Emulation Service Network Module Restrictions

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 vcmode, 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. The MCR is honored, however. 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
- Configuring SVCs for CES Operation

This section does not explain all possible ATM interface configuration options. For more information, see the sections "Configuring PVCs" and "Configuring SVCs" 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:

	Command	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.
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 signalling protocol between the router and the switch. To configure the ATM interface with SVCs, use the following commands beginning in global configuration mode:

	Command	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 signalling. 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 signalling 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` `Router(config-if)# svc [name] ces`	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.
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.

	Command	Purpose
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:

- Configuring Unstructured Circuit Emulation Service (Required)

or

- Configuring Structured Circuit Emulation Service (Required)
- Configuring Channel-Associated Signalling for Structured CES (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:

	Command	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.

	Command	Purpose
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:

	Command	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}`	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	`Router(config-controller)# framing {sf | esf}` or `Router(config-controller)# framing {crc4 | no-crc4} [australia]`	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}`	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.

	Command	Purpose
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 Signalling 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 signalling (CAS) information introduced into structured CES circuits by PBXs and time-division multiplexing (TDM) devices.

Note Only structured CES can support CAS.

The signalling supported depends on the WAN/voice interface card that is inserted in the CES deck. The signalling 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 signalling, first perform the tasks in the "Configuring Structured Circuit Emulation Service" section and then use the following commands beginning in global configuration mode:

	Command	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 signalling 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 timeslots. 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.
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:

	Command	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 OC-3/STM-1 ATM Circuit Emulation Service 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.

Command	Purpose
`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:

- Configuring Unstructured (Clear Channel) CES Services (Required)
- Configuring Structured (N x 64) CES Services (Required)

The following tasks are optional:

- Configuring Channel-Associated Signalling (for Structured CES Services Only) (Optional)
- Configuring Network Clock Source and Priorities (Optional)

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 "Configuring CES on an ATM-CES Port Adapter Example" 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:

	Command	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.
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:

	Command	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.
Step 5	`Router(config-if)# ces dsx1 linecode {ami | b8zs}` (for T1) or `Router(config-if)# ces dsx1 linecode {ami | hdb3}` (for E1)	Specifies the line code format used for the physical layer. The default is AMI.
Step 6	`Router(config-if)# ces dsx1 framing {esf | sf}` (for T1) or `Router(config-if)# ces dsx1 framing {e1_crc_mfCAS1t | e1_crc_mf_lt | e1_lt | e1_mfCAS_lt}` (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.
Step 9	`Router(config-if)# ces circuit circuit-number timeslots range`	Specifies the timeslots 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 timeslot (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.

	Command	Purpose
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.

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 Signalling (for Structured CES Services Only)

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 signalling (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 signalling bits. These signalling 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 signalling, first use the commands in the section "Configuring Structured (N x 64) CES Services" and then use the following commands beginning in global configuration mode:

	Command	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 signalling.
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" earlier in 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:

	Command	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.

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 "Configuring Network Clock Source Priority Example" at the end of this chapter.

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 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.

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

	Command	Purpose
Step 1	`Router(config-if)# atm pvp vpi [peak-rate]`	Creates a PVP and optionally specifies the peak rate.
Step 2	`Router(config-if)# pvc [name] vpi/vci`	(Optional) Creates a PVC with a VPI that matches the VPI specified in Step 1.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.

The value of the *vpi* argument is the virtual path identifier to be associated with the PVP (valid values are in the range 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.

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.

The **pvc** command is rejected if a non-multiplexed 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.

To display information about the PVP, use the **show atm vp** EXEC command.

Note If you change the peak rate online, the ATM port will go down and then back up.

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

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.

- Enabling the Serial Interface (Required)
- Enabling ATM-DXI Encapsulation (Required)
- Setting Up the ATM-DXI PVC (Required)
- Mapping Protocol Addresses to the ATM-DXI PVC (Required)
- Monitoring and Maintaining the ATM-DXI Serial Interface (Optional)

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

Enabling the Serial Interface

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

	Command	Purpose
Step 1	`Router(config)# interface serial number`	Enables the serial interface.
Step 2	`Router(config-if)# appletalk address network.node` or `Router(config-if)# ip address address mask` or `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.)

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.*

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.

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.

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.

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

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.

Repeat this task for each protocol to be carried on the PVC.

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 "ATM Access over a Serial Interface Example" later in this chapter.

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:

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

1. 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.[1]
`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.
`Router# show ima interface atm [slot]/ima [group-number] [detail]`	Displays general or detailed information about IMA groups and the links in those groups.

Command	Purpose
`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.

1. 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:

- Creating a PVC Example
- PVC with AAL5 and LLC/SNAP Encapsulation Examples
- PVCs in a Fully Meshed Network Example
- Configuring an ABR PVC Example
- Configuring PVC Discovery Example
- Enabling Inverse ARP Example
- Configuring Generation of End-to-End F5 OAM Loopback Cells Example
- Configuring PVC Trap Support Example
- Configuring Communication with the ILMI Example
- SVCs in a Fully Meshed Network Example
- ATM ESI Address Example
- ATM NSAP Address Example
- SVCs with Multipoint Signalling Example
- Configuring SVC Traffic Parameters Example
- Creating a VC Class Examples
- Applying a VC Class Examples
- ILMI Management on an ATM PVC Example
- OAM Management on an ATM PVC Example
- OAM Management on an ATM SVC Example
- Classical IP and ARP Examples
- Dynamic Rate Queue Examples
- PVC with AAL3/4 and SMDS Encapsulation Examples
- Transparent Bridging on an AAL5-SNAP PVC Example
- Inverse Multiplexing over ATM Examples
- Configuring ATM E.164 Auto Conversion Example

- Circuit Emulation Service Examples
- ATM Access over a Serial Interface Example
- ATM Port Adapters Connected Back-to-Back Example

Creating a PVC Example

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" and "Configuring PVC Traffic Parameters" earlier in this chapter.

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

PVC with AAL5 and LLC/SNAP Encapsulation Examples

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 1.1.1.1 with 1.1.1.5 at the other end of the connection. For further information, refer to the sections "Creating a PVC" and "Mapping a Protocol Address to a PVC" earlier in this chapter.

```
interface atm 3/0
 ip address 1.1.1.1 255.255.255.0
 pvc 0/50
 protocol ip 1.1.1.5 broadcast
 exit
!
 ip route-cache cbus
```

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

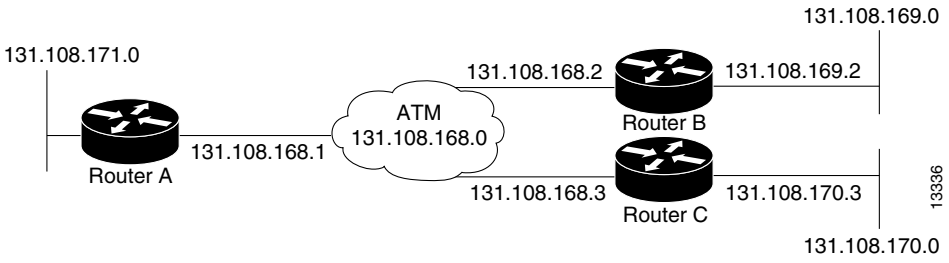
```
interface atm 4/0
 ip address 172.21.168.112 255.255.255.0
 atm maxvc 512
 pvc 1/51
 protocol ip 171.21.168.110
 exit
!
 pvc 2/52
 protocol decnet 10.1 broadcast
 exit
!
 pvc 3/53
 protocol clns 47.004.001.0000.0c00.6e26.00 broadcast
 exit
!
 decnet cost 1
 clns router iso-igrp comet
 exit
!
router 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
```

PVCs in a Fully Meshed Network Example

Figure 6 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" and "Mapping a Protocol Address to a PVC" earlier in this chapter.

Figure 6 Fully Meshed ATM Configuration Example



Router A

```
ip routing
!
interface atm 4/0
 ip address 131.108.168.1 255.255.255.0
 pvc 0/32
 protocol ip 131.108.168.2 broadcast
 exit
!
 pvc 0/33
 protocol ip 131.108.168.3 broadcast
 exit
```

Router B

```
ip routing
!
interface atm 2/0
 ip address 131.108.168.2 255.255.255.0
 pvc test-b-1 0/32
 protocol ip 131.108.168.1 broadcast
 exit
!
 pvc test-b-2 0/34
 protocol ip 131.108.168.3 broadcast
 exit
```

Router C

```
ip routing
!
```

```
interface atm 4/0
 ip address 131.108.168.3 255.255.255.0
 pvc 0/33
 protocol ip 131.108.168.1 broadcast
 exit
!
 pvc 0/34
 protocol ip 131.108.168.2 broadcast
 exit
```

Configuring an ABR PVC Example

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" earlier in this chapter.

```
interface atm 4/0
 ip address 1.1.1.1 255.255.255.0
 pvc 0/34
 atm abr rate-factor 32 32
 no shutdown
 exit
```

Configuring PVC Discovery Example

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" 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
```

Enabling Inverse ARP Example

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" earlier in this chapter.

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

Configuring Generation of End-to-End F5 OAM Loopback Cells Example

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 Generation of End-to-End F5 OAM Loopback Cells to Verify Connectivity" earlier in this chapter.

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

Configuring PVC Trap Support Example

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 171.69.61.90 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" section earlier in this chapter.

Configuring Communication with the ILMI Example

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" earlier in this chapter.

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

SVCs in a Fully Meshed Network Example

The following example is also a configuration for the fully meshed network shown in Figure 6, 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
- Configuring the NSAP Address
- Creating an SVC

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 131.108.168.3
 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
```

ATM ESI Address Example

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" earlier in this chapter.

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

ATM NSAP Address Example

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" 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.

SVCs with Multipoint Signalling Example

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

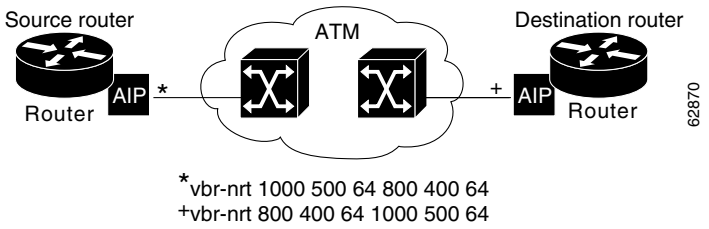
```
interface atm 2/0
 ip address 4.4.4.6 255.255.255.0
 pvc 0/5 qsaal
 exit
!
 pvc 0/16 ilmi
 exit
!
 atm esi-address 3456.7890.1234.12
!
 svc mcast-1 nsap cd.cdef.01.234566.890a.bcde.f012.3456.7890.1234.12 broadcast
 protocol ip 4.4.4.4 broadcast
 exit
!
 svc mcast-2 nsap 31.3233.34.352637.3839.3031.3233.3435.3637.3839.30 broadcast
 protocol ip 4.4.4.7 broadcast
 exit
!
 atm multipoint-signalling
 atm maxvc 1024
```

Configuring SVC Traffic Parameters Example

Figure 7 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" 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



Creating a VC Class Examples

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" and "Configuring VC Parameters" 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" and "Configuring VC Parameters" 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" and "Configuring VC Parameters" earlier in this chapter.

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

Applying a VC Class Examples

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" 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
```

ILMI Management on an ATM PVC Example

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" 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
```

OAM Management on an ATM PVC Example

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" earlier in this chapter.

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

OAM Management on an ATM SVC Example

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" 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
```

Classical IP and ARP Examples

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.

Configuring ATM ARP Client in an SVC Environment Example

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" 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
```

Configuring ATM ARP Server in an SVC Environment Example

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" 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
```

Configuring ATM Inverse ARP in a PVC Environment Example

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" 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.

Dynamic Rate Queue Examples

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" 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
```

PVC with AAL3/4 and SMDS Encapsulation Examples

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" 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.

Transparent Bridging on an AAL5-SNAP PVC Example

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 for SNAP PVCs" earlier in this chapter.

```
interface atm 4/0
 ip address 1.1.1.1 255.0.0.0
 pvc 1/33
 pvc 1/34
 pvc 1/35
 bridge-group 1
!
bridge 1 protocol dec
```

Inverse Multiplexing over ATM Examples

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

- E1 IMA on Multiport T1/E1 ATM Network Module Example
- T1 IMA on Multiport T1/E1 ATM Network Module Example
- T1 IMA on Multiport T1/E1 ATM Port Adapter Example

E1 IMA on Multiport T1/E1 ATM Network Module Example

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
```

T1 IMA on Multiport T1/E1 ATM Network Module Example

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 signalling. 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
```

T1 IMA on Multiport T1/E1 ATM Port Adapter Example

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 21.1.1.2 255.0.0.0
 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 signalling. 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 21.1.1.1 255.255.255.0
 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
!
!
```

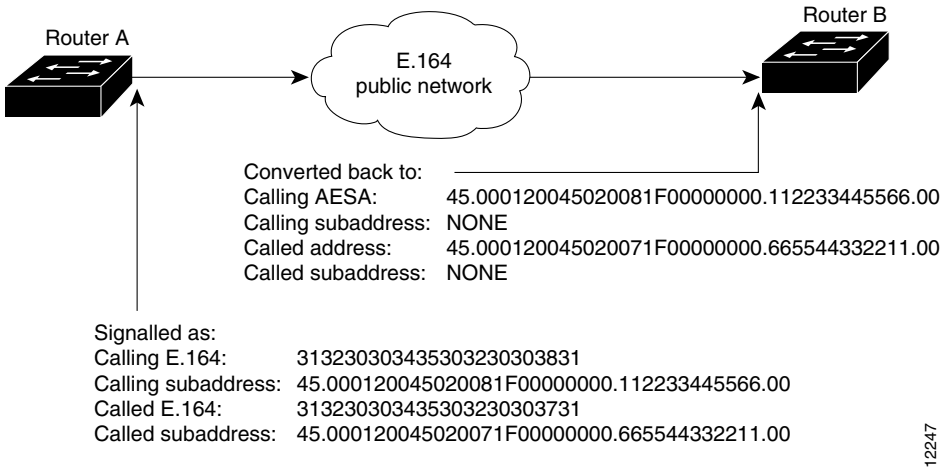
Configuring ATM E.164 Auto Conversion Example

The following example shows how to configure ATM E.164 auto conversion on an ATM interface. Figure 8 illustrates this example. For further information, refer to the section "Configuring ATM E.164 Auto Conversion Example" earlier in this chapter.

```
interface atm 0 multipoint
 ip address 120.45.20.81 255.255.255.0
 pvc 0/5 qsaal
 exit
```

```
!
 atm nsap-address 45.000120045020081F00000000.112233445566.00
 atm e164 auto-conversion
 svc nsap 45.000120045020071F00000000.665544332211.00
 protocol ip 120.45.20.71
 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.

Circuit Emulation Service Examples

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

- Configuring CES on an OC-3/STM-1 ATM Circuit Emulation Services Network Module Example
- Configuring CES on an ATM-CES Port Adapter Example
- Configuring Network Clock Source Priority Example
- Configuring Virtual Path Shaping Example

Configuring CES on an OC-3/STM-1 ATM Circuit Emulation Services Network Module Example

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 timeslots.

```
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 7.7.7.7 255.255.255.0
 no ip directed-broadcast
 no atm ilmi-keepalive
 pvc 1/101 ces
 pvc 1/200
  protocol ip 7.7.7.8 broadcast
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
ip route 0.0.0.0 0.0.0.0 172.18.193.1
ip route 12.0.0.0 255.0.0.0 1.1.1.1
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
```

Configuring CES on an ATM-CES Port Adapter Example

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" 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
```

Configuring Network Clock Source Priority Example

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" earlier in this chapter.

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

Configuring Virtual Path Shaping Example

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" earlier in this chapter.

```
interface atm 6/0
 ip address 2.2.2.2 255.255.255.0
 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
```

ATM Access over a Serial Interface Example

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
```

ATM Port Adapters Connected Back-to-Back Example

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
```

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

This chapter contains the following sections:

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.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the section "Identifying Supported Platforms" in the chapter "Using Cisco IOS Software."

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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 1 MPOA Message Flow Between MPCs and MPSs

The sequence of events shown in Figure 1 is 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

Table 1 lists and defines the MPOA terms used in Figure 1.

Table 1 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 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

Figure 1 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.

Figure 2 shows the relationships between MPC/MPS and LECs.

Figure 2 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 Figure 2, 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.

LAN Emulation Overview

This overview chapter gives a high-level description of LAN Emulation (LANE).

Procedures for configuring LANE are provided in the following chapters in this publication:

- "Configuring LAN Emulation" chapter
- "Configuring Token Ring LAN Emulation" chapter

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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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. Figure 1 illustrates the various virtual channel connections (VCCs)—also known as *virtual circuit connections*—that are used in LANE configuration.

Figure 1 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 1 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. Figure 2 illustrates a scenario in which one ELAN is set up on the switch and routers. Figure 3 illustrates a scenario in which several ELANs are 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.

Figure 2 illustrates this single ELAN configured across several routers.

Figure 2 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 Figure 3.

Figure 3 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.

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.

This chapter contains these sections:

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.

To identify the hardware platform or Cisco IOS image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the Cisco IOS release notes for a specific release. For more information, see the section "Identifying Supported Platforms" in the chapter "Using Cisco IOS Software."

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

The following sections contain information relevant to implementation:

- Network Support
- Hardware Support
- Addressing
- Rules for Assigning Components to Interfaces and Subinterfaces

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 server* 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" 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" and the "Multiple Token Ring ELANs with Restricted Membership Example" 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. Table 1 indicates how the values of unspecified digits are determined when an ATM address template is used:

Table 1 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)
ESI (next 6 bytes)	Filled with the slot MAC address[1] plus • 0—LANE client • 1—LES • 2—LANE BUS • 3—LECS
Selector field (last 1 byte)	Subinterface number, in the range 0 through 255.

1. 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.

To configure LANE, perform the tasks described in the following sections:

- Creating a LANE Plan and Worksheet
- Configuring the Prefix on the Switch
- Setting Up the Signalling and ILMI PVCs
- Displaying LANE Default Addresses
- Entering the LECS's ATM Address on the Cisco Switch
- Setting Up the LECS's Database
- Enabling the LECS
- Setting Up LESs and Clients

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

Although the sections described contain information about configuring SSRP fault tolerance, refer to the "Configuring Fault-Tolerant Operation" 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" section.

For configuration examples, see the "LANE Configuration Examples" 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.

To set the ATM address prefix on the Cisco LightStream 1010 Switch, use the following commands on the switch beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# atm-address {atm-address | prefix...}`	Sets the local node ID (prefix of the ATM address).
Step 2	`Router(config)# exit`	Exits global configuration mode.
Step 3	`Router# copy system:running-config nvram:startup-config`	Saves the configuration values permanently.

To set the ATM address prefix on the Cisco LightStream 100, use the following commands on the Cisco switch:

	Command	Purpose
Step 1	`Router(config-route-map)# set local name ip-address mask prefix`	Sets the local node ID (prefix of the ATM address).
Step 2	`Router(config-route-map)# save`	Saves the configuration values permanently.

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.

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:

	Command	Purpose
Step 1	`Router(config-if)# interface atm slot/0` `Router(config-if)# interface atm slot/port-adapter/0` `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's 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.

Depending on which type of switch you are using, perform one of the tasks in the following sections:

- Entering the ATM Addresses on the Cisco LightStream 1010 ATM Switch
- Entering the ATM Addresses on the Cisco LightStream 100 ATM Switch

Entering the ATM Addresses on the Cisco 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:

	Command	Purpose
Step 1	`Router(config)# atm lecs-address-default` *lecsaddress* `[`*sequence #*`]`[1]	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.

1. Refer to the *LightStream 1010 ATM Switch Command Reference* for further information about this command.

To enter the LECS addresses on the Cisco LightStream 1010 ATM switch per port, use the following commands beginning in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# atm lecs-address` *lecsaddress* `[`*sequence #*`]`[1]	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.

1. 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:

	Command	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's 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.

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 Only
- Setting Up the Database for Unrestricted-Membership Emulated LANs
- Setting Up the Database for Restricted-Membership LANs

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.

To set up the LECS for the default ELAN, use the following commands beginning in global configuration mode:

	Command	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.
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.

In Step 2, enter the ATM address of the server for the specified ELAN, as noted in your worksheet and obtained in the "Displaying LANE Default Addresses" 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 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" section later in this chapter.

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 configure a router as the LECS for multiple emulated LANs with unrestricted membership, use the following commands beginning in global configuration mode:

	Command	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. 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.

	Command	Purpose
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.

In the preceding steps, enter the ATM address of the server for the specified ELAN, as noted in your worksheet and obtained in the "Displaying LANE Default Addresses" section.

To set up fault-tolerant operation, see the "Configuring Fault-Tolerant Operation" section later in this chapter.

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 the LECS for emulated LANs with restricted membership, use the following commands beginning in global configuration mode:

	Command	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.

	Command	Purpose
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.
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.

To set up fault-tolerant operation, see the "Configuring Fault-Tolerant Operation" section later in this chapter.

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:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/0[.subinterface-number]` `Router(config)# interface atm slot/port-adapter/0[.subinterface-number]` `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.

	Command	Purpose
Step 3	`Router(config-if)# lane config auto-config-atm-address` `Router(config-if)# lane config auto-config-atm-address` or `Router(config-if)# lane config fixed-config-atm-address` `Router(config-if)# lane config fixed-config-atm-address` `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.
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, BUS, and a Client on a Subinterface
- Setting Up Only a Client on a Subinterface

Setting Up the Server, BUS, and a Client on a Subinterface

To set up the server, BUS, and (optionally) clients for an ELAN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **interface atm** *slot***/0.***subinterface-number* Router(config)# **interface atm** *slot/port-adapter***/0.***subinterface-number* 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*[1]	Provides a protocol address for the client.
Step 5	Router(config-if)# **Ctrl-Z**	Returns to EXEC mode.
Step 6	Router# **copy system:running-config nvram:startup-config**	Saves the configuration.

1. 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.

If the ELAN in Step 3 is intended to have *restricted membership*, 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.

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" section, before you set up the client.

To set up only a client for an emulated LANs, use the following commands beginning in interface configuration mode:

	Command	Purpose
Step 1	Router(config)# **interface atm** *slot***/0.***subinterface-number* Router(config)# **interface atm** *slot***/***port-adapter***/0.***subinterface-number* 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*[1]	Provides a protocol address for the client on this subinterface.
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.

1. 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.

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.

Disabling the LE_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. 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.

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.

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's ATM Address on the Cisco Switch" 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's Database" 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 command to 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.
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.

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*]	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.
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

The examples in the following sections describe how to configure LANE for the following cases:

- Default Configuration for a Single Ethernet ELAN Example
- Default Configuration for a Single Ethernet ELAN with a Backup LECS and LES Example
- Multiple Token Ring ELANs with Unrestricted Membership Example
- Multiple Token Ring ELANs with Restricted Membership Example
- TR-LANE with 2-Port SRB Example
- TR-LANE with Multiport SRB Example
- Routing Between Token Ring and Ethernet Emulated LANs Example

- Disabling LANE Flush Process Example

All examples use the automatic ATM address assignment method described in the "Method of Automatically Assigning ATM Addresses" section earlier in this chapter. These examples show the LANE configurations, not the process of determining the ATM addresses and entering them.

Default Configuration for a 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
```

Default Configuration for a 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 Figure 1. This example does not restrict membership in the emulated LANs.

Figure 1 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 Table 2 (the ESI part of the ATM address is derived from the first MAC address of the AIP shown in the example).

Table 2 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 Figure 2, 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 2 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 Figure 3. This example does not restrict membership in the emulated LANs.

Figure 3 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 Figure 4. 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 4 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
```

Routing Between Token Ring and Ethernet Emulated LANs Example

This example, shown in Figure 5, 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 5 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 47.009181000000001007385101.0050A2FEBC43.00
 lane client ethernet 100 elan1
!
line con 0
line vty 0 4
 no login
!
end
```

MQC Policy Map Support on Configured VC Range ATM

First Published: February 28, 2006
Last Updated: November 20, 2009

The Modular Quality of Service Command Line Interface (MQC) Policy Map support on Configured VC Range ATM feature extends the functionality for policy maps on a single ATM VC to the ATM VC range.

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 MQC Policy Map Support on Configured VC Range ATM" section on page 8.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About MQC Policy Map Support on Configured VC Range ATM

The MQC Policy Map Support on Configured VC Range feature simplifies the configuration of ATM VC ranges by allowing you to attach policy maps on a range of ATM VCs or on a specific VC within a range of VCs.

How to Configure MQC Policy Map Support on Configured VC Range ATM

To configure MQC policy maps on ATM VC ranges, perform the following configuration tasks:

- Attaching QoS Policies to an ATM PVC Range, page 2
- Attaching QoS Policies to an Individual PVC Within an ATM PVC Range, page 4

Attaching QoS Policies to an ATM PVC Range

Use the following configuration steps to attach a QoS policy to a range of ATM PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot/subslot/port*[*.subinterface*] [**multipoint** | **point-to-point**]
4. **range** [*range-name*] **pvc** *start-vpi/start-vci end-vpi/end-vci*
5. **service-policy** [**input** | **output**] *policy-map-name*
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** `slot/subslot/port[.subinterface]` [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 1/0.1`	Specifies the ATM interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**range** [*range-name*] **pvc** *start-vpi*/*start-vci* *end-vpi*/*end-vci* **Example:** `Router(config-if)# range pvc 101/304 200/400`	Defines a range of ATM permanent virtual circuits (PVCs) and enters ATM range configuration mode. • (Optional) *range-name* is the name of the range. The *range-name* can be a maximum of 15 characters. • *start-vpi*/ specifies the beginning value for a range of virtual path identifiers (VPIs). The slash is required. If you do not provide a VPI value or the slash, the default value of 0 is used. Valid values for VPI are from 0 to 255. • *start-vci* specifies the beginning value for a range of virtual channel identifiers (VCIs). Valid values are from 32 to 65535. • *end-vpi*/ specifies the end value for a range of virtual path identifiers (VPIs). The slash is required. If you do not provide a VPI value or the slash, the *start-vpi* value is used by default. Valid values for VPI are from 0 to 255. • *end-vci* specifies the end value for a range of virtual channel identifiers (VCIs). Valid values are from 32 to 65535.
Step 5	**service-policy** [**input** | **output**] *policy-map-name* **Example:** `Router(config-if-atm-range)# service-policy output Downstream_Traffic`	Attaches the service policy you specify to the specified ATM PVC range and enters ATM PVC range configuration mode. • **input** indicates to apply the service policy to the inbound traffic on the interface. • **output** indicates to apply the service policy to the outbound traffic on the interface. **Note** For QoS policies containing the **bandwidth**, **priority**, **random-detect**, **queue-limit**, and **shape** commands, you must specify the **output** keyword. The router ignores these commands when you use them with the **input** keyword. • *policy-map-name* is the name of the policy map you want to attach to the subinterface. **Note** The router applies the service policy to only the PVCs within the PVC range.
Step 6	**end** **Example:** `Router(config-if-atm-range)# end`	Exits ATM PVC range configuration mode and returns to privileged EXEC mode.

Attaching QoS Policies to an Individual PVC Within an ATM PVC Range

Use the following configuration task to attach a QoS policy to an individual PVC within a range of ATM PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot*/*subslot*/*port*[.*subinterface*] [**multipoint** | **point-to-point**]
4. **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*
5. **pvc-in-range** [*pvc-name*] *vpi*/*vci*
6. **service-policy** [**input** | **output**] *policy-map-name*
7. **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** slot/subslot/port[.subinterface] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 1/0`	Specifies the ATM interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**range** [*range-name*] **pvc** *start-vpi*/*start-vci* *end-vpi*/*end-vci* **Example:** `Router(config-if)# range pvc 101/304 200/400`	Defines a range of ATM permanent virtual circuits (PVCs) and enters ATM range configuration mode. • (Optional) *range-name* is the name of the range. The *range-name* can be a maximum of 15 characters. • *start-vpi*/ specifies the beginning value for a range of virtual path identifiers (VPIs). The slash is required. If you do not provide a VPI value or the slash, the default value of 0 is used. Valid values for VPI are from 0 to 255. • *start-vci* specifies the beginning value for a range of virtual channel identifiers (VCIs). Valid values are from 32 to 65535. • *end-vpi*/ specifies the end value for a range of virtual path identifiers (VPIs). The slash is required. If you do not provide a VPI value or the slash, the *start-vpi* value is used by default. Valid values for VPI are from 0 to 255. • *end-vci* specifies the end value for a range of virtual channel identifiers (VCIs). Valid values are from 32 to 65535.
Step 5	**pvc-in-range** [pvc-*name*] *vpi*/*vci* **Example:** `Router(config-if-atm-range)# pvc-in-range pvc 105/350`	Configures an individual PVC within a PVC range and enters ATM PVC range configuration mode. • (Optional) *pvc-name* is the name given to the PVC. The PVC name can have a maximum of 15 characters. • *vpi*/ is the virtual path identifier (VPI) for this PVC. The slash is required. If you do not specify a VPI value or the slash, the default value of 0 is used. Valid VPI values are from 0 to 255. • *vci* is the virtual circuit identifier (VCI) for this PVC. Valid values are from 32 to 2047.

	Command or Action	Purpose
Step 6	**service-policy** [**input** | **output**] *policy-map-name* **Example:** `Router(cfg-if-atm-range-pvc)# service-policy output Downstream_Rate`	Attaches the service policy you specify to the specified PVC within the ATM PVC range. • **input** indicates to apply the service policy to the inbound traffic on the interface. • **output** indicates to apply the service policy to the outbound traffic on the interface. **Note** For QoS policies containing the **bandwidth**, **priority**, **random-detect**, **queue-limit**, and **shape** commands, you must specify the **output** keyword. The router ignores these commands when you use them with the **input** keyword. • *policy-map-name* is the name of the policy map you want to attach to the subinterface. **Note** The router applies the service policy to only the individual ATM PVC within the PVC range.
Step 7	**end** **Example:** `Router(cfg-if-atm-range-pvc)# end`	Exits ATM PVC range configuration mode and enters privileged EXEC mode.

Configuration Examples for MQC Policy Map Support on Configured VC Range ATM

This section provides the following configuration examples:

- Attaching QoS Service Policies to a Range of ATM PVCs: Example, page 6
- Attaching QoS Service Policies to an Individual PVC Within a Range of ATM PVCs: Example, page 7

Attaching QoS Service Policies to a Range of ATM PVCs: Example

The following example configuration shows how to attach policy maps to a range of ATM PVCs. In the example, the service policy named voice is attached to the range of ATM PVCs 1/32 to 1/34. The router applies the service policy to all of the PVCs within the PVC range.

```
Router(config)# interface atm 2/0/0
Router(config-if)# range pvc 1/32 1/34
Router(config-if-atm-range)# service-policy input voice
```

Attaching QoS Service Policies to an Individual PVC Within a Range of ATM PVCs: Example

The following example configuration shows how to attach policy maps to a specific PVC within a PVC range. In the example, the service policy named data is attached to PVC 1/33 within the PVC range 1/32 to 1/34. The router applies the service policy to only PVC 1/33.

```
Router(config)# interface atm 2/0/0
Router(config-if)# range pvc 1/32 1/34
Router(config-if-atm-range)# service-policy input voice
Router(config-if-atm-range)# pvc-in-range 1/33
Router(config-if-atm-range-vc)# service-policy input data
```

Additional References

The following sections provide references related to MQC Policy Map Support on Configured VC Range.

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*
ATM PVC configuration	*Cisco IOS Asynchronous Transfer Mode Configuration Guide*
MQC policy maps	*Modular Quality of Service Command-Line Interface* feature
QOS Commands	*Cisco IOS Quality of Service Solutions Command Reference*
QOS Features	*Cisco IOS Quality of Service Solutions Configuration Guide*

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

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 MQC Policy Map Support on Configured VC Range ATM

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for MQC Policy Map Support on Configured VC Range

Feature Name	Releases	Feature Information
MQC Policy Map Support on Configured VC Range ATM	12.2(28)SB 12.4(2)T 12.2(33)SRE	The Modular Quality of Service Command Line Interface (MQC) Policy Map support on configured VC range feature extends the functionality for policy maps on a single ATM VC to the ATM VC range. The following command was introduced or modified: **service-policy**

OAM Segment Endpoint

First Published: November 8, 2004
Last Updated: November 20, 2009

The OAM Segment Endpoint feature terminates segment Operation, Administration and Maintenance (OAM) cells arriving on the Layer 2 transport virtual circuit (VC). The OAM Segment Endpoint feature helps in checking the segment connectivity. This feature can be used with Any Transport over MPLS (AToM) and Layer 2 Tunnel Protocol Version 3 (L2TPv3).

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 OAM Segment Endpoint" section on page 9.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for OAM Segment Endpoint

This feature can be enabled under Layer 2 transport permanent virtual circuit (PVC) submode and virtual circuit (VC) class configuration mode.

Restrictions for OAM Segment Endpoint

The following restrictions apply to the OAM Segment Endpoint feature:

- The OAM attachment circuit (AC) segment endpoint configuration is applicable only in the case of Layer 2 transport virtual circuits (VCs)/virtual paths (VPs).
- In Cisco 7200 routers, by default the segment cells for VPs are handled in the provider edge (PE) and are not transported on the pseudowire transparently.
- In Cisco 12000 series Internet routers, the segment OAM cells in VCs with encapsulation ATM adaptation layer 5 (AAL5) are handled in the PE and are not transported on the pseudowire transparently.
- If OAM cell emulation is configured, OAM segment endpoint is redundant.

Information About OAM Segment Endpoint

To configure the OAM Segment Endpoint feature, you should understand the following concept:

- VP/VC Segment Endpoint, page 2

VP/VC Segment Endpoint

The Cisco 12000 series Internet router or Cisco 7200 router responds to the incoming segment cells, if the OAM Segment Endpoint feature is configured; otherwise they are transferred on the pseudowire.

Irrespective of whether the is feature is enabled or not, End OAM cells for both VPs and VCs are transferred on the pseudowire. To terminate End OAM cells, you need to enable OAM-emulation.

Figure 1 shows ATM transport over MPLS.

Figure 1 ATM Transport over MPLS

How to Configure OAM Segment Endpoint

See the following sections for tasks that use the **oam-ac segment endpoint** command to terminate the segment OAM cells on a VC:

- Configuring OAM Segment Endpoint, page 3 (required)
- Verifying OAM Segment Endpoint, page 4 (optional)

Configuring OAM Segment Endpoint

This feature coexists with OAM emulation for Layer 2 VCs. If OAM emulation is already enabled, segment endpoint configuration is redundant. On the Cisco 12000 series router, F4/F5 distributed Operations, Administration and Maintenance (dOAM) is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot/port.subinterface-number*
4. **pvc** *vpi/vci* **l2transport**
5. **oam-ac segment endpoint**
6. **encapsulation aal5**
7. **xconnect** *peer-router-id vcid* **encapsulation mpls**
8. **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** *slot/port.subinterface-number* **Example:** `Router(config)# interface atm1/1`	Enters ATM interface configuration mode.
Step 4	**pvc** *vpi/vci* **l2transport** **Example:** `Router(config-if)# pvc 0/100 l2transport`	Creates an ATM PVC and enters L2transport VC configuration mode.

	Command or Action	Purpose
Step 5	**oam-ac segment endpoint** **Example:** `Router(config-if-atm-l2trans-pvc)# oam-ac segment endpoint`	Terminates segment cells arriving on the Layer 2 transport VC.
Step 6	**encapsulation aal5** **Example:** `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`	Specifies ATM AAL5 encapsulation for the PVC. • Make sure you specify the same encapsulation type on the PE and CE routers.
Step 7	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** `Router(config-if-atm-l2trans-pvc)# xconnect 192.0.2.10 100 encapsulation mpls`	Binds the attachment circuit to a pseudowire VC.
Step 8	**end** **Example:** `Router(cfg-if-atm-l2trans-pvc-xconn)# end`	Exits L2transport VC configuration mode and returns to privileged EXEC mode

Verifying OAM Segment Endpoint

To verify whether the OAM Segment Endpoint feature is working correctly, use the following steps to monitor the segment cells (arriving on the Layer 2 transport VC) that are being terminated on ATM links in a network.

SUMMARY STEPS

1. **enable**
2. **show atm pvc** [**ppp** | [**interface atm** *interface-number*[*.subinterface*]] [*connection-name* | *vpi*/*vci* [**vaccess** [**detail**]] | *vci*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm pvc** [**ppp** | [**interface atm** *interface-number*[*.subinterface*]] [*connection-name* | *vpi*/*vci* [**vaccess** [**detail**]] | *vci*]] **Example:** `Router# show atm pvc 0/100`	Displays all ATM PVCs and traffic information.

Configuration Examples for OAM Segment Endpoint

This section contains the following configuration and verification examples:

OAM Segment Endpoint Configuration: Example

VC Layer 2 Transport

```
Router(config)# interface atm1/1
Router(config-if)# pvc 0/100 l2transport
Router(cfg-if-atm-l2trans-pvc)# oam-ac segment endpoint
Router(cfg-if-atm-l2trans-pvc)# end
```

VC-Class Configuration

```
Router(config)# vc-class atm test
Router(config-vc-class)# oam-ac segment endpoint
Router(config-vc-class)# end
```

The following is sample output for the **show running-config interface** command:

```
Router# show running-config interface atm1/1

Building configuration...

Current configuration : 177 bytes
!
interface ATM1/1
 no ip address
 no ip directed-broadcast
 atm pvp 40 l2transport
  oam-ac segment endpoint
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/100 l2transport
  oam-ac segment endpoint
end

Router# show running-config
Building configuration...

Current configuration : 4251 bytes
!

vc-class atm test
  oam-ac segment endpoint
  oam-pvc manage
!
```

Verification Examples

The following is sample output from the **show atm pvc** command. It provides the segment OAM cell configuration and status information.

```
Router# show atm pvc 12/122

VC 12/122 doesn't exist on interface ATM1/0 - cannot display
VC 12/122 doesn't exist on interface ATM1/1 - cannot display
ATM1/2.3: VCD: 7, VPI: 12, VCI: 122
UBR, PeakRate: N/A (UBR VC)
AAL5 L2transport, etype:0xF, Flags: 0x10000C2E, VCmode: 0x0
OAM Cell Emulation: not configured
OAM Segment Endpoint: enabled
============> oam-ac segment endpoint enabled
Interworking Method: Not Configured
Remote Circuit Status = No Alarm, Alarm Type = None
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
Out CLP=1 Pkts: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0,
F5 InEndcc: 0, F5 InSegcc: 0, F5 InAIS: 0, F5 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0,
F5 OutEndcc: 0, F5 OutSegcc: 0, F5 OutAIS: 0, F5 OutRDI: 0
OAM cell drops: 0
Status: UP


Router# show atm pvc 40/3

ATM1/1: VCD: 48, VPI: 40, VCI: 3
UBR, PeakRate: N/A (UBR VC)
AAL5-MUX, etype:0x0, Flags: 0xD2C, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 0 second(s) OAM up retry count: 0, OAM
down retry count: 0 OAM Segment Endpoint: enabled OAM END CC Activate retry count: 0, OAM
END CC Deactivate retry count: 0 OAM END CC retry frequency: 0 second(s), OAM SEGMENT CC
Activate retry count: 0, OAM SEGMENT CC Deactivate retry
count: 0
OAM SEGMENT CC retry frequency: 0 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: Not Managed
OAM SEGMENT CC status: OAM CC Ready
OAM SEGMENT CC VC state: Not Managed
InARP DISABLED
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
Out CLP=1 Pkts: 0
OAM cells received: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutAIS: 0, F4 OutRDI: 0 OAM cell drops: 0
Status: UP
```

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	*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[1]	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*

1. 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

Feature Information for OAM Segment Endpoint

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for OAM Segment Endpoint

Feature Name	Releases	Feature Information
OAM Segment Endpoint	12.0(30)S 12.2(33)SRE	The OAM Segment Endpoint feature terminates segment Operation, Administration and Maintenance (OAM) cells arriving on the Layer 2 transport virtual circuit (VC). The OAM Segment Endpoint feature helps in checking the segment connectivity. This feature can be used with Any Transport over MPLS (AToM) and Layer 2 Tunnel Protocol Version 3 (L2TPv3). The following sections provide information about this feature: • VP/VC Segment Endpoint, page 2 • Configuring OAM Segment Endpoint, page 3 The following commands were introduced or modified: **oam-ac segment endpoint, show atm pvc**.

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.

ATM OAM Ping

First Published: December 15, 2001
Last Updated: November 20, 2009

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 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 the ATM OAM Ping Feature" section on page 9.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

To use the ATM OAM Ping feature, you must understand the following concepts:

- Benefits of the ATM OAM Ping Feature, page 2
- How to Use the ATM OAM Ping Feature, page 3

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

The following sections describe tasks that use **ping** commands to test network connectivity in an ATM network:

- Testing Network Connectivity Using ATM Interface Ping in the Normal Mode, page 3 (optional)
- Testing Network Connectivity Using ATM Interface Ping in the Interactive Mode, page 3 (optional)
- Aborting a Ping Session, page 4 (optional)

Testing Network Connectivity Using ATM Interface Ping in the 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 ATM Interface Ping in the 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 STEP

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
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 the ATM OAM Ping Feature

This section provides the following configuration examples:

- Verifying the Connectivity of a Specific PVC: Example, page 4
- Testing Network Connectivity Using ATM Interface Ping in the Normal Mode: Example, page 5
- Testing Network Connectivity Using ATM Interface Ping in the Interactive Mode: Example, page 6

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 ATM Interface Ping in the 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 ATM Interface Ping in the 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 Feature

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 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**

ATM Multilink PPP Support on Multiple VCs

First Published: November 25, 2002
Last Updated: November 20, 2009

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 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 ATM Multilink PPP Support on Multiple VCs" section on page 15.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for ATM Multilink PPP Support on Multiple VCs

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 on Multiple VCs

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 on Multiple VCs

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 on Multiple VCs

This section contains the following tasks:

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.
Step 9	**ppp multilink fragment disable** **Example:** `Router(config-if)# ppp multilink fragment disable`	Disables packet fragmentation.

	Command or Action	Purpose
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

Perform this task to define 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:** `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	**no ip address** **Example:** `Router(config-if)# no ip address`	Removes existing IP addresses or disables IP processing.

	Command or Action	Purpose
Step 5	**load-interval** *seconds* **Example:** `Router(config-if)# load-interval 30`	Changes the length of time for which data is used to compute load statistics.
Step 6	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables MLP on the interface.
Step 7	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink-group 44`	Restricts a physical link to joining only a designated multilink-group interface.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Defining the PVCs and Making Them Bundle Member Links

Perform this task to define the PVCs and make them bundle member links.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot*/**0**

   or

   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:** `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*/**0** or **interface atm** *slot*/*port* **Example:** `Router(config)# interface atm 2/0` or `Router(config)# interface atm 2/1`	Specifies the ATM interface type and enters interface configuration mode.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Removes an IP address or disables IP processing.
Step 5	**load interval** *seconds* **Example:** `Router(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:** `Router(config-if)# atm ilmi-keepalive`	Enables Interim Local Management Interface (ILMI) keepalives.
Step 7	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(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:** `Router(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:** `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. • 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:** `Router(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:** `Router(config-if)# end`	Exits interface configuration mode.

Verifying ATM Multilink PPP Support on Multiple VCs

Perform this task to display information about ATM Multilink PPP Support on Multiple VCs:

SUMMARY STEPS

1. **enable**
2. **show frame-relay pvc** [[**interface** *interface*] [*dlci*] [**64-bit**] | **summary** [**all**]]
3. **show interfaces**
4. **show policy-map**
5. **show ppp multilink**
6. **show queueing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm pvc** **Example:** `Router# show atm pvc`	Displays all ATM PVCs and traffic information.
Step 3	**show frame-relay pvc** [[**interface** *interface*] [*dlci*] [**64-bit**]	**summary** [**all**]] **Example:** `Router# show frame-relay pvc 16`	Displays statistics about PVCs for Frame Relay interfaces.
Step 4	**show interfaces** **Example:** `Router# show interfaces`	Displays interleaving statistics. • Interleaving data is displayed only if interleaving occurs.

	Command or Action	Purpose
Step 5	**show policy-map** **Example:** `Router# 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:** `Router# show ppp multilink`	Displays bundle information for the MLP bundles and their PPP links in the router.
Step 7	**show queueing** **Example:** `Router# show queueing`	Lists all or selected configured queueing strategies.

Monitoring ATM Multilink PPP Support on Multiple VCs

Perform this task to monitor ATM Multilink PPP Support on Multiple VCs.

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug atm errors** **Example:** `Router# debug atm errors`	Displays ATM errors.
Step 3	**debug atm events** **Example:** `Router# debug atm events`	Displays ATM events.

	Command or Action	Purpose
Step 4	**debug ppp error** **Example:** `Router# debug ppp error`	Displays information on traffic and exchanges in an internetwork implementing the PPP.
Step 5	**debug ppp multilink events** **Example:** `Router# debug ppp multilink events`	Displays information about events affecting multilink groups.
Step 6	**debug voice RTP** **Example:** `Router# 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 on Multiple VCs

This section provides the following configuration examples:

- Defining the Service Policy Using the MQC Configuration: Example, page 11
- Defining a Multilink MLP Bundle Interface Configuration: Example, page 11
- Defining Virtual Templates for Member Links Configuration: Example, page 12
- Defining PVCs and Making Them Bundle Member Links Configuration: Example, page 12

Defining the Service Policy Using the MQC Configuration: Example

The following example shows how to configure a service policy using the MQC:

```
Router> enable
Router# configure terminal
Router(config)# class-map match-all DATA
Router(config-cmap)# match ip precedence 0
Router(config-cmap)# class-map match-all VOICE
Router(config-cmap)# match access-group 100
Router(config-cmap)# policy-map CISCO
Router(config-pmap)# class VOICE
Router(config-pmap-c)# priority percent 70
Router(config-pmap-c)# class DATA
Router(config-pmap-c)# bandwidth percent 5
Router(config-pmap-c)# access-list 100 permit udp any any precedence critical
```

Defining a Multilink MLP Bundle Interface Configuration: Example

The following example shows how to define a multilink bundle for the mulitilink interface:

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface Multilink1
Router(config-if)# ip address 10.2.1.1 255.0.0.0
Router(config-if)# load-interval 30
Router(config-if)# no cdp enable
Router(config-if)# service-policy output CISCO
Router(config-if)# ppp multilink fragment disable
Router(config-if)# ppp multilink group 1
```

Defining Virtual Templates for Member Links Configuration: Example

The following example shows how to define virtual templates for member links:

```
Router> enable
Router# configure terminal
Router(config)# interface Virtual-Template1
Router(config-if)# no ip address
Router(config-if)# load-interval 30
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 1
Router(config-if)# interface Virtual-Template2
Router(config-if)# no ip address
Router(config-if)# load-interval 30
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 1
```

Defining PVCs and Making Them Bundle Member Links Configuration: Example

The following example shows how to define and configure PVCs as bundle members:

```
Router> enable
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# no ip address
Router(config-if)# load-interval 30
Router(config-if)# atm ilmi-keepalive
Router(config-if)# pvc 0/34
Router(config-if-atm-vc)# vbr-nrt 1536 1536
Router(config-if-atm-vc)# tx-ring-limit 5
Router(config-if-atm-vc)# protocol ppp Virtual-Template1
Router(config-if-atm-vc)# pvc 0/35
Router(config-if-atm-vc)# vbr-nrt 800 800
Router(config-if-atm-vc)# tx-ring-limit 3
Router(config-if-atm-vc)# protocol ppp Virtual-Template2
Router(config-if-atm-vc)# pvc 0/36
Router(config-if-atm-vc)# vbr-nrt 800 400 94
Router(config-if-atm-vc)# tx-ring-limit 5
Router(config-if-atm-vc)# protocol ppp Virtual-Template1
Router(config-if-atm-vc)# pvc 0/37
Router(config-if-atm-vc)# vbr-nrt 800 800
Router(config-if-atm-vc)# tx-ring-limit 3
Router(config-if-atm-vc)# protocol ppp Virtual-Template2
Router(config-if-atm-vc)# end
```

Additional References

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 List: 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 List: 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*

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
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 on Multiple VCs

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 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	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.

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.

Local Template-Based ATM PVC Provisioning

First Published: February 3, 2003
Last Updated: November 20, 2009

The Local Template-Based ATM Provisioning feature enables ATM permanent virtual circuits (PVCs) to be provisioned automatically as needed from a local configuration. ATM PVC autoprovisioning can be configured on a PVC, an ATM PVC range, or a virtual cicuit (VC) class. If a VC class configured with ATM PVC autoprovisioning is assigned to an interface, all the PVCs on that interface will be autoprovisioned; this configuration is sometimes referred to as an *infinite range*.

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 Local Template-Based ATM PVC Provisioning, page 13.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for Local Template-Based ATM PVC Provisioning

The number of PVCs that can be established on an interface that is configured as an infinite range is limited to the maximum number of VCs that the platform can support.

Information About Local Template-Based ATM PVC Provisioning

Autoprovisioned ATM PVCs are not created until there is activity on the virtual path identifier (VPI)/virtual channel identifier (VCI) pair. When the interface is disabled and reenabled using the **shutdown** and **no shutdown** commands, autoprovisioned PVCs that are part of a PVC range or infinite range are removed upon shutdown and are not reestablished until the first incoming packet triggers PVC creation. During router reload, autoprovisioned PVCs are created when there is activity on the connection.

The total number of VCs that can be configured on an ATM port adapter is limited by the capacity of port adapter. In cases of ATM link oversubscription, where a PVC range or infinite range is configured to provision more PVCs than the port adapter allows, the PVCs can be configured with a timeout so that they can be dynamically brought down as needed. When the timeout expires, the idle PVCs are removed, allowing the PVC range or infinite range of PVCs to share system resources.

ATM PVC local autoprovisioning supports the following applications: PPP over ATM, PPP over Ethernet, ATM routed bridge encapsulation, and routed RFC 1483.

The Local Template-Based ATM Provisioning feature enables ATM PVCs to be created automatically as needed from a local configuration, making the provisioning of large numbers of digital subscriber line (DSL) subscribers easier, faster, and less prone to error.

How to Configure Local Template-Based ATM PVC Provisioning

This section contains the following tasks:

- Configuring ATM PVC Local Autoprovisioning in a VC Class (required)
- Configuring ATM PVC Local Autoprovisioning on a PVC (required)
- Configuring ATM PVC Local Autoprovisioning on an ATM PVC Range (required)
- Configuring ATM PVC Local Autoprovisioning on PVC Within a Range (required)
- Verifying ATM PVC Autoprovisioning (required)
- Monitoring and Maintaining ATM PVC Local Autoprovisioning (optional)

Configuring ATM PVC Local Autoprovisioning in a VC Class

Perform this task to enable ATM PVC local autoprovisioning in a VC class. A VC class configured with ATM PVC autoprovisioning can be assigned to an ATM interface, an ATM PVC, an ATM PVC range, and an ATM PVC with a range.

Note If a VC class that is configured with ATM PVC autoprovisioning is assigned to an ATM interface, all PVCs on the interface will be autoprovisioned.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **create on-demand**
5. **idle-timeout** *seconds* [*minimum-rate*]
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	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm vctest`	Creates a VC class for an ATM PVC, SVC, or ATM interface and enters ATM VC class configuration mode.
Step 4	**create on-demand** **Example:** `Router(config-vc-class)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.
Step 5	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-vc-class)# idle-timeout 10`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 6	**end** **Example:** `Router(config-vc-class)# end`	Returns to privliged EXEC mode.

Configuring ATM PVC Local Autoprovisioning on a PVC

Perform this task to enable ATM PVC local autoprovisioning on a PVC. ATM PVC local autoprovisioning can also be configured on a PVC by assigning a VC class that has been configured with ATM PVC local autoprovisioning to the PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot*/*port*
4. **atm autovc retry** *interval*
5. **pvc** [*name*] *vpi*/*vci*
6. **create on-demand**
7. **idle-timeout** *seconds* [*minimum-rate*]
8. **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** *slot*/*port* **Example:** `Router(config)# interface atm 2/0`	Configures an ATM interface and enters interface configuration moed.
Step 4	**atm autovc retry** *interval* **Example:** `Router(config-if)# atm autovc retry 32`	(Optional) Configures the interval at which the router will repeat the attempt to create autoprovisioned PVCs after a failure of the initial creation attempt.
Step 5	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(config-if)# pvc vctest 32/3`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 6	**create on-demand** **Example:** `Router(config-if-atm-vc)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.

	Command or Action	Purpose
Step 7	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-if-atm-vc)# idle-timeout 12`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 8	**end** **Example:** `Router(config-if-atm-vc)# end`	Returns to privileged EXEC mode.

Configuring ATM PVC Local Autoprovisioning on an ATM PVC Range

Perform this task to enable ATM PVC autoprovisioning on an ATM PVC range. ATM PVC local autoprovisioning can also be configured on a range by assigning a VC class that has been configured with ATM PVC local autoprovisioning to the range.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot*/*port*
4. **atm autovc retry** *interval*
5. **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*
6. **create on-demand**
7. **idle-timeout** *seconds* [*minimum-rate*]
8. **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** *slot*/*port* **Example:** `Router(config)# interface atm 2/0`	Configures an ATM interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**atm autovc retry** *interval* **Example:** `Router(config-if)# atm autovc retry 12`	(Optional) Configures the interval at which the router will repeat the attempt to create autoprovisioned PVCs after a failure of the initial creation attempt.
Step 5	**range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci* **Example:** `Router(config-if)# range pvc pvctest 2/3 4/6`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 6	**create on-demand** **Example:** `Router(config-if-atm-range)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.
Step 7	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-if-atm-range)# idle-timeout 12`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 8	**end** **Example:** `Router(config-if-atm-range)# end`	Returns to privileged EXEC mode.

Configuring ATM PVC Local Autoprovisioning on PVC Within a Range

Perform this task to enable ATM PVC autoprovisioning on a PVC within an ATM PVC range. ATM PVC local autoprovisioning can also be configured on a PVC within a range by assigning a VC class that has been configured with ATM PVC local autoprovisioning to the PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot*/*port*
4. **atm autovc retry** *interval*
5. **range** [**range-name**] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*
6. **pvc-in-range** [*pvc-name*] [[*vpi*/]*vci*]
7. **create on-demand**
8. **idle-timeout** *seconds* [*minimum-rate*]

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 2/0`	Configures an ATM interface and enters interface configuration mode.
Step 4	**atm autovc retry** *interval* **Example:** `Router(config-if)# atm autovc retry 23`	(Optional) Configures the interval at which the router will repeat the attempt to create autoprovisioned PVCs after a failure of the initial creation attempt.
Step 5	**range** [range-name] **pvc** *start-vpi*/*start-vci* *end-vpi*/*end-vci* **Example:** `Router(config-if)# range range1 pvc 2/4 5/6`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 6	**pvc-in-range** [*pvc-name*] [[*vpi*/]*vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range pvc1`	Defines an individual PVC within a PVC range and enables PVC-in-range configuration mode.
Step 7	**create on-demand** **Example:** `Router(config-if-atm-range-pvc)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.
Step 8	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-if-atm-range-pvc)# idle-timeout 10`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 9	**end** **Example:** `Router(config-if-atm-range-pvc)# end`	Returns to privileged EXEC mode.

Verifying ATM PVC Autoprovisioning

Perform this task to verify if ATM PVC local autoprovisioning is configured and working correctly.

Step 1 Enter the **show running-config** command to verify that the configuration is correct.

Step 2 Enter the **show atm pvc** command. PVCs that have been autoprovisioned will have the value “PVC-A” (“A” stands for automatic) in the Type field.

```
Router# show atm pvc

            VCD /                                          Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC     Kbps   Kbps   Cells  Sts
5/0.1       117        0     50   PVC-A   SNAP    UBR  149760                UP
5/0.1       118        0     51   PVC-A   SNAP    UBR  149760                UP
5/0.1       119        0     52   PVC-A   SNAP    UBR  149760                UP
```

Step 3 Enter the **show atm pvc** command with the *vpi*/*vci* arguments to see if ATM PVC local autoprovisioning is configured on a specific PVC. If ATM PVC local autoprovisioning is configured, the text “VC Auto Creation Enabled: local” will appear in the output.

```
Router# show atm pvc 0/51

ATM5/0.1: VCD: 118, VPI: 0, VCI: 51
UBR, PeakRate: 149760
AAL5-LLC/SNAP, etype:0x0, Flags: 0x20000C20, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 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
ILMI VC state: Not Managed
InARP frequency: 15 minutes(s)
Transmit priority 4
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 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 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
PPP: Virtual-Access3 from Virtual-Template1
VC Auto Creation Enabled: local
```

Monitoring and Maintaining ATM PVC Local Autoprovisioning

To monitor and maintain ATM PVC autoprovisioning, use one or more of the following commands in privileged EXEC mode:

Command or Action	Purpose
`Router# debug atm autovc {event | error | all}`	Displays information about autoprovisioned ATM PVC events and errors.
`Router# show atm pvc`	Displays all ATM PVCs and traffic information.
`Router# show atm vc`	Displays all ATM PVCs and SVCs and traffic information.

Configuration Examples for Local Template-Based ATM PVC Provisioning

This section provides the following configuration examples:

- ATM PVC Local Autoprovisioning on an ATM Interface Example
- ATM PVC Local Autoprovisioning on a PVC Example
- ATM PVC Local Autoprovisioning on an ATM PVC Range Example
- ATM PVC Local Autoprovisioning on a PVC Within a Range Example

ATM PVC Local Autoprovisioning on an ATM Interface Example

In the following example, local autoprovisioning is enabled on all PVCs on ATM interface 5/0.

```
vc-class atm auto-pppoe
 vbr-nrt 1000 100
 protocol pppoe
 create on-demand
 idle-timeout 300 10
!
interface atm 5/0
 class-int auto-pppoe
 atm autovc retry 10
```

ATM PVC Local Autoprovisioning on a PVC Example

The following example shows the configuration of local autoprovisioning on a PVC:

```
interface atm 5/0
 pvc 1/300
  create on-demand
  idle-timeout 300 10
```

ATM PVC Local Autoprovisioning on an ATM PVC Range Example

The following example shows the configuration of local autoprovisioning on an ATM PVC range called "auto":

```
interface atm 5/0
 range auto pvc 0/100 1/200
  create on-demand
```

ATM PVC Local Autoprovisioning on a PVC Within a Range Example

The following example shows the configuration of local autoprovisioning on a PVC within a PVC range:

```
interface atm 5/0
 range auto pvc 0/100 1/200
  pvc-in-range 0/101
   create on-demand
```

Additional References

The following sections provide references related to the Local Template-based ATM PVC Provisioning feature.

Related Documents

Related Topic	Document Title
ATM PVC configuration	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*
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

Feature Information for Local Template-Based ATM PVC Provisioning

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(15)B, Cisco IOS Releases 12.2(28)SB, Cisco IOS Release 12.2(33)SRE or Cisco IOS Release 15.0(1)M, or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Local Template-Based ATM PVC Provisioning

Feature Name	Releases	Feature Information
Local Template-Based ATM PVC Provisioning	12.2(15)B 15.0(1)M 12.2(28)SB 12.2(33)SRE	The Local Template-Based ATM Provisioning feature enables ATM permanent virtual circuits (PVCs) to be provisioned automatically as needed from a local configuration. This feature was introduced in Cisco IOS Release 12.2(15)B and integrated into Cisco IOS Release 12.2(28)SB, Cisco IOS Release 15.0(1)M and Cisco IOS Release 2.2(33)SRE. The following commands were introduced or modified: **atm autovc retry**, **create on-demand**, **debug atm autovc**, **idle-timeout**

Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

First Published: February 3, 2003
Last Updated: November 20, 2009

The Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature enhances PPP over ATM (PPPoA)/PPP over Ethernet (PPPoE) autosense functionality by providing autosense support on multiplexer (MUX) and Subnetwork Access Protocol (SNAP)-encapsulated ATM permanent virtual circuits (PVCs).

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 Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs" section on page 11.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

- Do not use this feature on a router that initiates PPPoA sessions.
- This feature supports ATM PVCs. Switched virtual circuits (SVCs) are not supported.
- PPPoA does not support static IP assignments within virtual templates.

Information About Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

PPPoA/PPPoE autosense enables a router to distinguish between incoming PPPoA and PPPoE over ATM sessions and to create virtual access based on demand for both PPP types.

This feature is supported on MUX- and SNAP-encapsulated ATM PVCs and enables the PVC encapsulation type to be autosensed by the router. The router determines the encapsulation type of a PVC by looking at the encapsulation type of the first incoming packet. If the PVC encapsulation type is changed while the PPPoA or PPPoE session on the network access server (NAS) is still up, the incoming packet is dropped, the encapsulation type is reset to autosense, and all sessions are removed from the PVC. The next incoming packet will then determine the new encapsulation type of the PVC.

Benefits of Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

The Autosense of PPPoA/PPPoE for MUX or SNAP Encapsulation feature provides resource allocation on demand. For each PVC configured for both PPPoA and PPPoE, certain resources (including one virtual-access interface) are allocated upon configuration, regardless of the existence of a PPPoA or PPPoE session on that PVC. With the Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature, resources are allocated for PPPoA and PPPoE sessions only when a client initiates a session, thus reducing overhead on the NAS.

This feature also saves configuration time by eliminating the need to specify the encapsulation type when provisioning ATM PVCs and by eliminating the need to manually provision ATM PVCs each time the encapsulation type changes.

How to Configure PPPoA/PPPoE Autosense on ATM PVCs

This section contains the following tasks:

- Verifying PPPoA/PPPoE Autosense Configuration, page 5 (optional)
- Monitoring and Maintaining PPPoA/PPPoE Autosense for ATM PVCs, page 6 (optional)

Configuring PPPoA/PPPoE Autosense

Perform this task to configure PPPoA/PPPoE Autosense on a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*[**.***subinterface-number* {**multipoint** | **point-to-point**}]
4. **pvc** [*name*] *vpi*/*vci*
5. **encapsulation aal5autoppp virtual-template** *number*
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** *number*[**.***subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 2/0.2 multipoint`	Specifies the ATM interface and optional subinterface and enters subinterface configuration mode.
Step 4	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(config-subif)# pvc pvc1 45/54`	Configures a PVC on the ATM interface or subinterface and enters interface-ATM-VC configuration mode.

	Command or Action	Purpose
Step 5	**encapsulation aal5autoppp virtual-template** *number* **Example:** `Router(config-if-atm-vc)# encapsulation aal5autoppp virtual-template 3`	Configures PPPoA/PPPoE autosense on the PVC. • Also specifies the virtual template interface to use to clone the new virtual-access interfaces for PPP sessions on this PVC.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Ends the session and enters privileged EXEC mode.

Configuring PPPoA/PPPoE Autosense on a VC Class

Perform this task to configure PPPoA/PPPoE autosense on a VC class.

Note Virtual-access interfaces for PPPoE sessions are cloned from the virtual template interface specified in the VPDN group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **encapsulation aal5autoppp virtual-template** *number*
5. **exit**
6. **interface atm** *number*[**.***subinterface-number* {**multipoint** | **point-to-point**}]
7. **class-int** *vc-class-name*
8. **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.

	Command or Action	Purpose
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm vc1`	Creates and names a map class.
Step 4	**encapsulation aal5autoppp virtual-template** *number* **Example:** `Router(config-vc-class)# encapsulation aal5autoppp virtual-template 4`	Configures PPPoA/PPPoE autosense. • Also specifies the virtual template interface to use to clone the new virtual-access interfaces for PPP sessions on this PVC.
Step 5	**exit** **Example:** `Router(config-vc-class)# exit`	Returns to global configuration mode.
Step 6	**interface atm** *number*[**.***subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface 2/0.2 multipoint`	Specifies the ATM interface enters subinterface configuration mode.
Step 7	**class-int** *vc-class-name* **Example:** `Router(config-subif)# class-int vc1`	Applies the VC class to all VCs on the ATM interface or subinterface.
Step 8	**end** **Example:** `Router(config-subif)# end`	Ends the session and enters privileged EXEC mode.

Verifying PPPoA/PPPoE Autosense Configuration

To verify that you have successfully configured PPPoA/PPPoE autosense, use the **show running-config** command in 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.

Monitoring and Maintaining PPPoA/PPPoE Autosense for ATM PVCs

Perform this task to monitor and maintain PPPoA/PPPoE autosense.

SUMMARY STEPS

1. **enable**
2. **show atm pvc** [**ppp**]
3. **show caller**
4. **show interface virtual** *interface-number*
5. **show user**
6. **show vpdn**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm pvc** [**ppp**] **Example:** `Router# show atm pvc ppp`	After the client at the other end of the PVC has initiated a PPPoA session, use this command to check that the PVC contains the PPPoA session.
Step 3	**show caller** **Example:** `Router# show caller`	Displays caller information. Use this command to: • View individual users and consumed resources on the NAS. • Inspect active call statistics for large pools of connections. (The **debug** commands produce too much output and tax the CPU too heavily.) • Display the absolute and idle times for each user. The current values for both of these settings are displayed on the tty line and the asynchronous interface. Users that have been idle for unacceptably long periods of time can be easily identified. By using this information, you can define time out policies and multiple grades of services for different users.

	Command or Action	Purpose
Step 4	**show interface virtual** *interface-number* **Example:** `Router# show interface virtual access 1`	Displays information about the virtual-access interface, LCP[1], protocol states, and interface statistics. • The status of the virtual-access interface should read: `Virtual-Access3 is up, line protocol is up`
Step 5	**show user** **Example:** `Router# show user`	Displays information about the active lines on the router.
Step 6	**show vpdn** **Example:** `Router# show vpdn`	Displays information about active Level 2 Forwarding (L2F) Protocol tunnel and message identifiers in a VPDN[2].

1. LCP = link control protocol.
2. VPDN = virtual private dial-up network.

Configuration Examples for Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

This section provides the following configuration examples:

PPPoA/PPPoE Autosense on an ATM PVC: Example

The following example shows how to configure the NAS with PPPoA/PPPoE autosense on PVC 30/33:

```
! Configure PPP Autosense
!
interface ATM 0/0/0.33 multipoint
 pvc 30/33
 encapsulation aal5autoppp Virtual-Template1
!
! Configure PPPoE
!
vpdn enable
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
!
ip cef
interface virtual-template 1
 ip unnumbered fastethernet 0/0/0
 ip route-cache cef
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
```

```
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
```

PPPoA/PPPoE Autosense on a VC Class: Example

The following example shows how to configure the NAS with PPPoA/PPPoE autosense on the VC class called ‘MyClass’. The ‘MyClass’ VC class applies PPPoA/PPPoE autosense to all PVCs on the ATM 0/0/0.99 interface:.

```
! Configure PPP Autosense
!
vc-class ATM MyClass
 encapsulation aal5autoppp Virtual-Template1
!
interface ATM 0/0/0.99 multipoint
  class-int MyClass
  no ip directed-broadcast
  pvc 20/40
  pvc 30/33
!
! Configure PPPoE
!
vpdn enable
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
!
ip cef
interface virtual-template 1
  ip unnumbered fastethernet 0/0/0
  ip route-cache cef
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
```

PPPoA/PPPoE Autosense on Multiple VC Classes and Virtual Templates: Example

The following example shows how to handle PPPoA and PPPoE sessions separately by two virtual templates:

```
ip cef
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
pppoe limit per-mac 1
pppoe limit per-vc 1
!
```

```
virtual-template 1 pre-clone 1500
virtual-template 2 pre-clone 1000
!
interface ATM0/0/0.3 multipoint
 no ip directed-broadcast
 class-int pppauto
!
interface ATM0/0/0.9 multipoint
 ip address 10.16.40.1 255.255.0.0
 no ip directed-broadcast
!
interface Virtual-Template1
 ip unnumbered ATM0/0/0.9
 ip route-cache cef
 no ip directed-broadcast
 peer default ip address pool pool-1
 ppp authentication pap
!
interface Virtual-Template2
 ip unnumbered ATM0/0/0.9
 ip route-cache cef
 no ip directed-broadcast
 peer default ip address pool pool-2
 ppp authentication chap
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
!
vc-class atm pppauto
 encapsulation aal5autoppp Virtual-Template2
!
```

Note Whenever possible, it is preferable to configure PPPoA and PPPoE to use the same virtual template. Using separate virtual templates leads to the inefficient use of virtual access because the maximum number of virtual-access interfaces will have to be precloned twice: once for PPPoE and once for PPPoA. If PPPoA and PPPoE use the same virtual template, the maximum number of virtual-access interfaces can be precloned once and used for PPPoA and PPPoE as needed.

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*

Related Topic	Document Title
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

Feature Information for Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

Feature Name	Releases	Feature Information
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	12.2(15)B 12.2(28)SB 12.2(33)SRE	The Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature enhances PPP over ATM (PPPoA)/PPP over Ethernet (PPPoE) autosense functionality by providing autosense support on MUX- and SNAP-encapsulated ATM permanent virtual circuits (PVCs). The following commands were introduced or modified: **encapsulation aal5autoppp virtual-template**

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.

Configuring ATM PVC F5 OAM Recovery Traps

First Published: August 26, 2003
Last Updated: November 20, 2009

The ATM PVC F5 OAM Recovery Traps feature introduces Simple Network Management Protocol (SNMP) traps that notify the administrator when a permanent virtual circuit (PVC) has recovered from F5 Operation, Administration, and Maintenance (OAM) end-to-end loopback failures, and F5 OAM alarm indication signal/remote defect indication (AIS/RDI) failures.

The ATM PVC TRAP Enhancement for Segment and End AIS / RDI failures feature adds Segment and End AIS/RDI Failure notification (traps) to the existing ATM PVC trap infrastructure.

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 Configuring ATM PVC F5 OAM Recovery Traps" section on page 11.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Configuring ATM PVC F5 OAM Recovery Traps

- Extended ATM PVC up and down traps and ATM PVC traps for OAM F5 Continuity Check (CC), OAM F5 AIS/RDI, and OAM F5 loopback failures and recoveries cannot be used at the same time as legacy ATM PVC traps.
- Legacy ATM PVC traps must be disabled by using the **no snmp-server enable traps atm pvc** command before before extended ATM PVC up and down traps and ATM PVC traps for OAM F5 CC, OAM F5 AIS/RDI, and OAM F5 loopback failures and recoveries 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 legacy ATM PVC traps.
- OAM management must be enabled on the PVC before you can use any ATM PVC traps.

Restrictions for Configuring ATM PVC F5 OAM Recovery Traps

- The F5 OAM recovery traps are supported for ATM PVCs only.
- The CISCO-ATM-PVCTRAP-EXTN-MIB is currently supported in Cisco IOS Release 12.0(27)S, Cisco IOS Release 12.2(33)SRE, Cisco IOS Release 15.0(1)M and later releases.
- The traps associated with CC are supported only on Cisco IOS 7500 series routers with PA-A3 and PA-A1 cards and Gigabit Switch Router (GSR).

Information About Configuring ATM PVC F5 OAM Recovery Traps

To configure ATM PVC F5 OAM recovery traps, you should understand the following concepts:

F5 OAM Recovery Traps for ATM PVCs

F5 OAM cells are used to detect connectivity failures and recoveries at the ATM layer. Before the introduction of this feature, Cisco IOS software provided support for SNMP traps (also called SNMP notifications) for F5 end-to-end loopback, and F5 AIS/RDI connectivity failures on a PVC. The ATM PVC F5 OAM Recovery Traps feature introduces SNMP traps that notify the network management system (NMS) when connectivity is restored to a PVC after the following types of failures:

- F5 OAM end-to-end loopback failures
- F5 OAM segment AIS/RDI failures
- F5 OAM end-to-end AIS/RDI failures

Information in the traps includes the number of PVCs that recovered and time stamps indicating when the first and last recoveries occurred during the notification interval.

To limit the amount of traffic that can be generated by the F5 OAM failure and recovery traps, only one trap of each type can be generated in each trap interval. Each trap can report on multiple PVCs, and successive PVCs that have the same failure or recovery are reported as a range.

In addition to the traps, MIB tables are maintained to provide information about the failures and recoveries on PVCs.

For a complete description of the extended ATM PVC TRAP MIB, including the supported notifications and tables, see the MIB file called CISCO-ATM-PVCTRAP-EXTN-MIB.my, available through Cisco.com at the following URL:

http://www.cisco.com/go/mibs

Benefits of F5 OAM Recovery Traps for ATM PVCs

Before the introduction of this feature, when F5 OAM failures were detected on PVCs, failure notifications were sent to the NMS, and the operational state of the PVC was kept up. There was no mechanism for notifying the NMS when connectivity was restored to the PVCs after F5 OAM failures. The F5 OAM Recovery Traps feature introduces traps that asynchronously notify the NMS when PVCs have recovered from F5 OAM failures.

ATM PVC Trap Enhancements for Segment and End AIS/RDI Failures

ATM PVC trap support provides ATM PVC failure notification by sending a trap when a PVC on an ATM interface fails or leaves the UP operational state. F5 OAM cells are used to detect connectivity failures and recoveries at the ATM layer. The operator informs the NMS of these OAM failures using ATM PVC traps. The following ATM PVC Traps are supported:

- ATM PVC DOWN TRAP
- ATM PVC F5 Loop back failure TRAP
- ATM PVC F5 Segment CC failure TRAP
- ATM PVC F5 End-to-End CC failure TRAP
- ATM PVC F5 AIS/RDI failure TRAP

When connectivity is restored, the PVC state is brought UP for allowing data transfer to take place over the PVC. This connectivity restoration uses the OAM cells. The following recovery traps are used to inform the NMS about the restoration of connectivity:

- ATM PVC UP TRAP
- ATM PVC F5 Loop back recovery TRAP
- ATM PVC F5 Segment CC recovery TRAP
- ATM PVC F5 End-to-End CC recovery TRAP
- ATM PVC F5 AIS/RDI recovery TRAP

To limit the amount of traffic that can be generated by the F5 OAM failure and recovery traps, only one trap of each type can be generated in each trap interval. Each trap can report on multiple PVCs, and successive PVCs that have the same failure or recovery are reported as a range.

The ATM PVC Trap Enhancements for Segment and End AIS/RDI failures feature addresses the issue of generating the separate ATM F5 segment and end AIS/RDI failure and recovery traps.

Benefits of the ATM PVC Trap Enhancements for Segment and End AIS/RDI Failures Feature

The ATM PVC TRAP Enhancement for Segment and End AIS/RDI Failures feature adds segment and end AIS/RDI Failure notification (traps) to the existing ATM PVC trap infrastructure. This feature adds the ifDescr object to the existing traps. The addition of this object allows the operator to get the interface name directly from the trap. The segment and end AIS/RDI failure and recovery traps are generated when AIS/RDI failure traps are enabled.

How to Configure F5 OAM Recovery Traps for ATM PVCs

This section contains the following procedures:

- Configuring ATM OAM Support, page 4
- Enabling OAM F5 Failure and Recovery Traps for ATM PVCs, page 5

Configuring ATM OAM Support

Perform this task to configure ATM OAM 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** [**keep-vc-up** [**end aisrdi failure** | **seg aisrdi failure**]]
7. **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.

	Command or Action	Purpose
Step 3	**interface atm** *number* **Example:** `Router(config)# interface atm 0`	Specifies an interface for configuration and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.3 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(config-if)# pvc 0/40`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 6	**oam-pvc manage** [**keep-vc-up** [**end aisrdi failure** | **seg aisrdi failure**]] **Example:** `Router(config-if-atm-vc)# oam-pvc manage`	Configures ATM OAM management.
Step 7	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM virtual circuit configuration mode.

Enabling OAM F5 Failure and Recovery Traps for ATM PVCs

Perform this task to enable the MIB and SNMP notifications that support ATM OAM F5 CC management.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps atm pvc extension** {**up** | **down** | **oam failure** [**aisrdi** | **loopback**]}
4. **end**

DETAILED STEPS

	Command	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** | **loopback** } **Example:** `Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi`	Enables ATM OAM F5 AIS/RDI failure and recovery traps and ATM OAM F5 end-to-end loopback failure and recovery traps.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Troubleshooting Tips

- Use the **show running-config** command to verify the configuration of ATM OAM management.
- Use the **show atm pvc** command to verify that ATM OAM management is enabled and to display the state of the PVC.
- Use the **debug snmp packet** command to display which SNMP traps are being generated.

Configuration Examples for Configuring ATM PVC F5 OAM Recovery Traps

Enabling OAM PVC Managment: Example

The following example shows how to enable ATM PVC OAM management:

```
Router(config)# interface ATM 2/0.1 point-to-point
Router(config-subif)# pvc pvc 45/54
Router(config-if-atm-vc)# oam-pvc manage
Router(config-if-atm-vc)# end
```

Note Enhanced Interior Gateway Routing Protocol (EIGRP) must be configured on the router if you want the notification packets to be sent to the NMS.

ATM PVC Extended Up and Down Notifications: Examples

Enabling ATM PVC Extended Up and Down Notifications

The following example shows how to enable ATM PVC extended up and down notifications:

```
Router(config)# snmp-server community public RW
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server host 10.0.0.115 vrf Mgmt-intf version 2c public udp-port 2030
```

ATM PVC Down Notification

The following sample output shows an ATM PVC in the DOWN state:

```
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
0/3/0.100  pvc100         0   100 PVC     SNAP       UBR  149760              DN

Received SNMPv2c Trap:
Community: public
From: 10.0.0.54
sysUpTimeInstance = 1918435
snmpTrapOID.0 = catmIntfPvcDownTrap
ifIndex.52 = 52
atmIntfPvcFailures.15 = 4
atmIntfCurrentlyFailingPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
catmPVclCurFailTime.52.0.100 = 1915435
catmPVclPrevRecoverTime.52.0.100 = 259552
catmPVclFailureReason.52.0.100 = catmLoopbackOAMFailure(1)
```

ATM PVC Up Notification

The following sample output shows an ATM PVC in the UP state:

```
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
0/3/0.100  pvc100         0   100 PVC     SNAP       UBR  149760              UP

Received SNMPv2c Trap:
Community: public
From: 9.0.0.54
sysUpTimeInstance = 1933376
snmpTrapOID.0 = catmIntfPvcUp2Trap
ifIndex.52 = 52
catmIntfCurrentlyDownToUpPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
catmPVclCurRecoverTime.52.0.100 = 1930676
```

```
catmPVclPrevFailTime.52.0.100 = 1915435
catmPVclRecoveryReason.52.0.100 = catmLoopbackOAMRecover(1)
```

ATM OAM Failure Looback Notification: Examples

Enabling ATM OAM Failure Loopback Notification

The following example shows how to enable ATM PVC OAM failure loopback notifications and extended up and down notifications:

```
Router(config)# snmp-server community public RW
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server host 10.0.0.115 vrf Mgmt-intf version 2c public udp-port 2030
```

Note If you configure the **snmp-server enable traps atm pvc extension oam failure** command, you may not see up or down traps when an OAM failure trap is generated. Additionally, the PVC will stay in the UP state.

OAM Loopback Failure Notification

The following sample output shows an ATM PVC that has failed. Note that the output indicates the PVC is still in the UP state.

```
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
0/3/0.100  pvc100         0   100 PVC     SNAP       UBR  149760              UP

Received SNMPv2c Trap:
Community: public
From: 9.0.0.54
sysUpTimeInstance = 1964155
snmpTrapOID.0 = catmIntfPvcOAMFailureTrap
ifIndex.52 = 52
catmIntfOAMFailedPVcls.15 = 65
catmIntfCurrentOAMFailingPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
catmPVclStatusTransition.52.0.100 = 1
catmPVclStatusChangeStart.52.0.100 = 1961155
catmPVclStatusChangeEnd.52.0.100 = 1961155
```

OAM Loopback Recovery Notification

The following sample output shows an ATM PVC in the UP state:

```
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
0/3/0.100  pvc100         0   100 PVC     SNAP       UBR  149760              UP


Received SNMPv2c Trap:
Community: public
```

```
From: 9.0.0.54
sysUpTimeInstance = 1986456
snmpTrapOID.0 = catmIntfPvcOAMRecoverTrap
ifIndex.52 = 52
catmIntfOAMRcovedPVcls.15 = 10
catmIntfCurrentOAMRcovingPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
catmPVclStatusUpTransition.52.0.100 = 1
catmPVclStatusUpStart.52.0.100 = 1983456
catmPVclStatusUpEnd.52.0.100 = 1983456
```

Additional References

The following sections provide references related to ATM PVC OAM F5 recovery traps.

Related Documents

Related Topic	Document Title
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

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
• ATM PVC MIB • CISCO-ATM-PVCTRAP-EXTN-MIB.my • CISCO-IETF-ATM2-PVCTRAP-MIB	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
No new or modified RFCs are supported by this features.	—

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 Configuring ATM PVC F5 OAM Recovery Traps

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.0(26)S, and Cisco IOS Release 15.0(1)M or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Configuring ATM PVC F5 OAM Recovery Traps

Feature Name	Releases	Feature Information
ATM PVC F5 OAM Recovery Traps	12.0(26)S 15.0(1)M	The ATM PVC F5 OAM Recovery Traps feature introduces SNMP traps that notify the administrator when a PVC has recovered from F5 OAM end-to-end loopback failures and F5 OAM AIS/RDI failures. The following sections provide information about this feature: • F5 OAM Recovery Traps for ATM PVCs, page 2 • Benefits of F5 OAM Recovery Traps for ATM PVCs, page 3 • Configuring ATM OAM Support, page 4 The following command was introduced: **snmp-server enable traps atm pvc extension**.
ATM PVC Trap Enhancements for Segment and End AIS/RDI Failures	12.0(27)S 15.0(1)M	The ATM PVC TRAP Enhancement for Segment and End AIS/RDI failures feature adds segment and end AIS/RDI failure notification (traps) to the existing ATM PVC trap infrastructure. The following sections provide information about this feature: • ATM PVC Trap Enhancements for Segment and End AIS/RDI Failures, page 3 • Benefits of the ATM PVC Trap Enhancements for Segment and End AIS/RDI Failures Feature, page 4 • Enabling OAM F5 Failure and Recovery Traps for ATM PVCs, page 5

802.1ah Support for Ethernet Infrastructure

First Published: November 20, 2009
Last Updated: November 20, 2009

The Excalibur MAC Tunneling Protocol (MTP) feature is based on IEEE 802.1ah standard and provides Virtual Bridged Local Area Network (VLAN) and MAC scalability. This feature extends the Cisco QinQ (IEEE 802.1ad) capability to support highly scalable Provider Backbone Bridge Architecture (PBB). MTP allows a service provider to interconnect multiple Provider Bridged Networks (PBNs) with maximum 10,48,576 (2 to the 20th power) Service VLANS support and extend the MAC address scalability.

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 802.1ah Support for Ethernet Infrastructure" section on page 12.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About 802.1ah Support for Ethernet Infrastructure

With this feature, you can scale a Provider Bridged P802.1ad network using the existing Bridged and VLAN deployment. Although the current Cisco QinQ capability provides for VLAN scaling, this feature extends the scaling and inter-operability between multiple vendors.

To make forwarding decisions, Bridges in a Provider Backbone Bridged Network (PBBN) need to learn MAC address of each host. MTP resolves the issue of MAC address learning by encapsulating the data packet and MAC addresses (source and destination) into a new Ethernet frame. The header of the new Ethernet frame contains:

- Destination Backbone MAC (B-MAC)
- Source Backbone MAC (B-MAC)
- Backbone VLAN TAG (B-TAG) with 12 bit Backbone VLAN ID (B-VID)
- Service Instance TAG (I-TAG) with 24 bit Service Instance ID (I-SID)

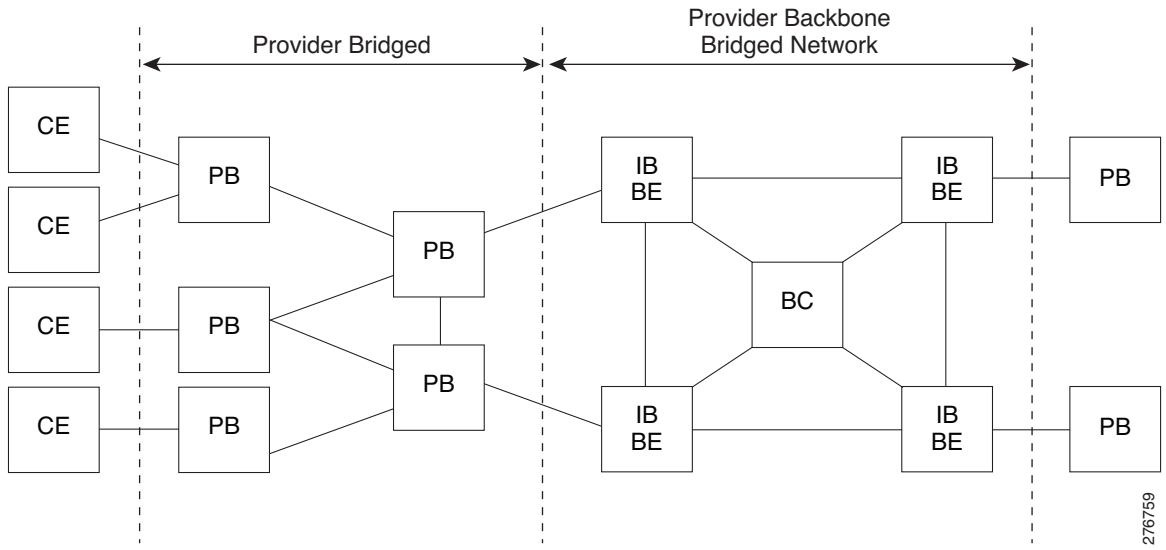
MAC scalability is implemented using the B-MACs. Since the new Ethernet frames are encapsulated with MAC address while traversing the PBBN, a bridge needs to learn only the B-MACs. The MAC addresses of hosts are hidden from the Provider Backbone Bridges (PBB), resulting in the PB Bridges to learn only the provider MAC address, independent of the number of hosts or the number of host MAC addresses supported. Since the data packets are sent to specific MAC addresses, the 802.1ah cloud is not flooded with unnecessary traffic. A MAC address may be a static entry in the MAC address table on the Backbone Core Bridge.

The VLAN scalability is implemented using the I-SID. The MTP achieves VLAN scalability by using a backbone VLAN TAG with 12 bit B-VID and the Service Instance TAG with 24 bit Service Instance ID to provide the VLAN scalability necessary to map large number of customers.

MTP Software Architecture

The encapsulation and de-capsulation of MAC addresses is performed on a Backbone Edge Bridge (BEB) at the edge of the PBBN. A BEB can be an I-Bridge (I-BEB), a B-bridge (B-BEB), or an IB-bridge (IB-BEB). MTP with IB-BEB functionality is also supported. Figure 1 shows the MTP software architecture:

Figure 1 MTP Software Architecture



IB Backbone Edge Bridge

The IB-BEB consists of one B-Component and one or more I-Components. An IB-BEB provides the functionality to select the B-MAC and insert I-SIDs based on the supported tags. It also validates the I-SIDs and transmits or receives the frames on the B-VLAN.

The 802.1ah draft describes two types of customer facing interfaces supported by IB-BEB:

- S-Tagged Service Interface
  - Translating S-tagged Interface
  - Bundling S-tagged interface
- Port Based (transparent) Service Interface

MTP supports these interfaces.

Data Plane Processing

The packets on the ingress EFP are tunneled to the appropriate MAC tunnel using the C-MAC bridge domain. For multiple EFPs using the same I-SID, the switching among EFPs is done using the C-MAC bridge domain. The local switching is performed across all the ports in the bridge domain even if they span multiple tunnel engines.

MTP Configuration

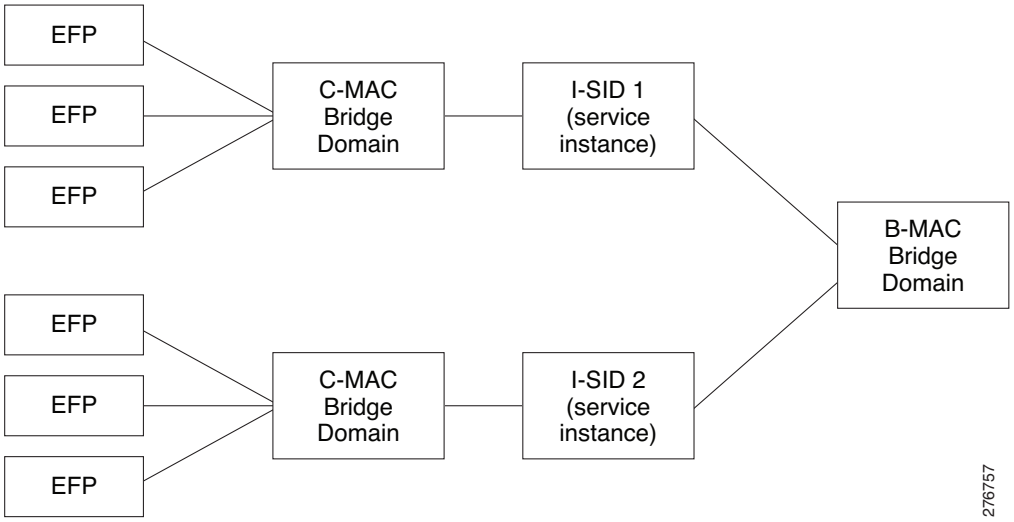
Table 1 lists the relationship between the various entities in a Cisco 7600 Series router for MTP implementation:

Table 1 Relationship between the various entities in a Cisco 7600 Series Router

Entity to Entity	Relationship
EFP to C-MAC bridge domain	many to one
C-MAC bridge domain to I-SID	one to one
I-SID to B-MAC bridge domain	many to one

Figure 2 show N to N relationship within a Cisco 7600 Series Router:

Figure 2 N to N relationship within a Cisco 7600 Series Router



Scalability Information

Table 2 lists the scalability information for MTP:

Table 2 Scalability Information for MTP

Scalability Factor	Scalability Number
Total number of EVCs in the system	32000
Total number of EVCs per line card	16000
Total number of ISIDs in the system	
Total C-MAC addresses per LC	128000 (32000 per NPU)
Total number of EVCs per ISID per NPU	110
Total number of EVCs per ISID for a two port Excalibur	220
Total number of EVCs per ISID for a four port Excalibur	440
Total B-bridge-domains per chassis	4094

Scalability Factor	Scalability Number
Total I-SIDs or MAC-Tunnels	16000
Total entries in a C-MAC table	32000

How to Configure 802.1ah Support for Ethernet Infrastructure

The configuration of 802.1ah support for ethernet infrastructure of Excalibur MTP for Cisco 7600 Router is described in detail below.

Restrictions

Follow these restrictions and usage guidelines when configuring the MAC Tunneling Protocol on an ES40 line card:

- By default, all the BPDUs are dropped.
- The Port channels with 802.1ah EVCs are supported. However, there can only be one member link per port channel.
- The IGMP Snooping or any multicast protocol support on the C bridge-domain.
- The MAC address synchronization and MAC address move notification in the C bridge-domain is not supported.
- The DHCP Snooping with 802.1ah EVCs is not supported.
- The B-Bridge and I-Bridge models are not supported.
- An ISID configured under a MAC-Tunnel cannot be configured on another MAC-Tunnel.
- The tunnel-engine configuration is not supported.
- Source MAC address configuration for a Tunnel-Engine is not supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitEthernet** *slot/port* or **interface tengigabitEthernet** *slot/port*
4. **service instance id** {**Ethernet** [*service-name*]}
5. **encapsulation untagged dot1q** {*any* | *vlan-id*[*vlan-id*[*vlan-id*]} **second-dot1q** {*any* |*vlan-id*[*vlan-id*[*vlan-id*]]}
6. **rewrite ingress tag** {**push {dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} [**symmetric**]
7. **bridge-domain bridge-id c-mac**
8. **exit**
9. **exit**
10. **ethernet mac-tunnel virtual mac-in-mac tunnel identifier**

11. **bridge-domain bridge-id**
12. **service instance id** {**Ethernet** [*service-name*]}
13. **encapsulation dot1ah i-sid i-sid_number**
14. **bridge-domain bridge-id c-mac**
15. **exit**
16. **exit**
17. **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 gigabitEthernet** *slot/port* or **interface tengigabitEthernet** *slot/port* **Example:** `Router(config)#interface GigabitEthernet 3/1`	Specifies the Gigabit Ethernet interface to be configured, where: • *slot/port*—Specifies the location of the interface
Step 4	**service instance id** {**Ethernet** [*service-name*]} **Example:** `Router(config-if)#service instance 20 ethernet`	Creates a service instance (an instance of an EVC) on an interface and sets the device into the config-if-srv mode.
Step 5	**encapsulation untagged dot1q** {*any* | *vlan-id*[*vlan-id*[*vlan-id*]} **second-dot1q** {*any* |*vlan-id*[*vlan-id*[*vlan-id*]]} **Example:** `Router(config-if-srv)#encapsulation dot1q 40 second-dot1q 42`	Configures the encapsulation. Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.

	Command or Action	Purpose
Step 6	**rewrite ingress tag** {**push {dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} [**symmetric**] [**no**] **bridge-domain bridge-id c-mac** **Example:** `Router(config-if-srv)#rewrite ingress tag pop 1 symmetric`	Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.
Step 7	**bridge-domain bridge-id c-mac** **Example:** `Router(config-if-srv)#bridge-domain 21 c-mac`	Configuring the bridge domain. Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.
Step 8	**exit** **Example:** `Router(config-if-srv)#exit`	Exits the service instance mode.
Step 9	**exit** **Example:** `Router(config-if)#exit`	Exits the interface mode.
Step 10	**ethernet mac-tunnel virtual mac-in-mac tunnel identifier** **Example:** `Router(config)#ethernet mac-tunnel virtual 22`	Configures mac-in-mac tunnel and creates a tunnel identifier for the 802.1ah cloud. Sets the configuration to config-tunnel-minm mode.
Step 11	**bridge-domain bridge-id** **Example:** `Router(config-tunnel-minm)#bridge-domain 200`	Binds the mac tunnel to the B-MAC bride domain instance.
Step 12	**service instance id** {**Ethernet** [*service-name*]} **Example:** `Router(config-tunnel-minm)#service in 23 ethernet`	Defines the service instance to be used with B-VLAN. Set the configuration mode to config-tunnel-srv mode.
Step 13	**encapsulation dot1ah i-sid i-sid_number** **Example:** `Router(config-tunnel-srv)#encapsulation dot1ah isid 24`	Defines the matching criteria to be used to map 802.1ah frames with I-SID id to the appropriate EVC.

	Command or Action	Purpose
Step 14	**bridge-domain bridge-id c-mac** **Example:** `Router(config-tunnel-srv)#bridge-domain 21 c-mac`	Maps the I-SID used for forwarding the customer packets to a specific EVC on the interface. The bridge-id mentioned step 7 must match with bridge-id in this step to ensure proper configuration.
Step 15	**exit** **Example:** `Router(config-tunnel-srv)#exit`	Exits the mac-tunnel service instance mode.
Step 16	**exit** **Example:** `Router(config-tunnel-minm)#exit`	Exits the mac-tunnel mode.
Step 17	**exit** **Example:** `Router(config)#exit`	Exits the global config mode.

Configuration Examples for 802.1ah Support for Ethernet Infrastructure

This example shows how to configure Excalibur MTP for Cisco 7600 Routers:

```
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet 3/1
Router(config-if)#service instance 20 ethernet
Router(config-if-srv)#encapsulation dot1q 40 second-dot1q 42
Router(config-if-srv)#rewrite ingress tag pop 1 symmetric
Router(config-if-srv)#bridge-domain 21 c-mac
Router(config-if-srv)#exit
Router(config-if)#exit
Router(config)#ethernet mac-tunnel virtual 22
Router(config-tunnel-minm)#bridge-domain 200
Router(config-tunnel-minm)#service in 23 ethernet
Router(config-tunnel-srv)#encapsulation dot1ah isid 24
Router(config-tunnel-srv)#bridge-domain 21 c-mac
Router(config-tunnel-srv)#exit
Router(config-tunnel-minm)#exit
Router(config)#exit
```

Use the following commands to verify the MTP configuration:

- You can use the **show platform mtp slot** *slot_num* command to verify the MTP configuration. This command shows the information about MTP for each slot:

```
Router#sh platform mtp slot 3
SLOT        TUNNELENGINE          VLAN_LIST
 3          MacTunnelEngine3/0      200
 3          MacTunnelEngine3/1
 3          MacTunnelEngine3/2
 3          MacTunnelEngine3/3
```

- You can use **show platform mtp c_bd** *c-vlan-id* to view information about a specific C-VLAN:

```
Router#sh platform mtp c_bd 21
C_BD        B_BD           SLOT       PPE          C_BD_COUNT
 21         200             3          0               1
Router#
```

- You can use **show platform mtp b_bd** *b-vlan-id* to view information about a specific B-VLAN:

```
Router#sh platform mtp b_bd 200
B_BD        SLOT           PPE        B_BD_COUNT
200          3              0             1
Router#
```

- You can use **show platform mtp befp** *b-efp-id* to view information about a specific B-EFP:

```
Router#sh platform mtp befp 23
BEFP       C_BD           B_BD        SLOT           PPE          C_BD_COUNT
23         21             200          3              0              1
Router#
```

- You can use **show ethernet service mac-tunnel summary** to view a summary of information about a specific mac tunnel.
- You can use **show ethernet service mac-tunnel** *id* [**detail**] to view information about a specific mac tunnel, and the ID can range from 1 to 4094.

```
Router#show ethernet service mac-tunnel 1 detail
Tunnel Id: 1
EFP Microblocks:
****************
Microblock type: Bridge-domain
Bridge-domain: 20

No. of Service Instances: 1

Service Instance ID: 16000
Associated Tunnel Id: 1
Encapsulation: dot1ah 1 vlan-type 0x88E7
Rewrite: egress tag push dot1ah 1 vlan-type 0x88E7 symmetric
State: Up
mac-tunnel address map: 0001.0001.0001 0002.0002.0002
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0
EFP Microblocks:
****************
Microblock type: Bridge-domain
Bridge-domain: 1 c-mac

Microblock type: CFM
CFM encapsulation:
```

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*

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

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.	—

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 802.1ah Support for Ethernet Infrastructure

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

.

Table 3 Feature Information for 802.1ah Support for Ethernet Infrastructure

Feature Name	Releases	Feature Information
802.1ah Support for Ethernet Infrastructure	12.2(33)SRE	The Excalibur MAC Tunneling Protocol (MTP) feature is based on 802.1ah standard and provides VLAN and MAC scalability. This feature extends the Cisco QinQ (IEEE 802.1ad) capability to support highly scalable PBA. In 12.2(33)SRE, this feature was introduced on the Cisco 7600. The following commands were introduced or modified: **service instance id**, **encapsulation untagged dot1q**, **rewrite ingress tag**, **bridge-domain bridge-id c-mac**, **ethernet mac-tunnel virtual mac-in-mac tunnel identifier**, **encapsulation dot1ah**, **bridge-domain bridge-id c-mac**, **show ethernet service mac-tunnel**.

Configuring ATM SNMP Trap and VC OAM Enhancements

First Published: August, 2001
Last Updated: November 20, 2009

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 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 Configuring ATM SNMP Trap and OAM VC Enhancements" section on page 13.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Configuring ATM SNMP Trap and VC 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 Configuring ATM SNMP Trap and VC 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 Configuring ATM SNMP Trap and VC 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 VC 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 VC OAM Enhancements

This section contains the following tasks:

- Configuring Extended ATM PVC Trap Support, page 5 (required)
- Enabling OAM Management, page 6 (required)
- Enabling OAM AIS-RDI Monitoring, page 8 (required)
- Verifying ATM PVC Traps (optional)

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. • **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. **interface atm** *slot*/**0**[.*subinterface-number* {**multipoint | point-to-point**}]

   or

   interface atm *slot*/*port-adapter*/**0**[**.***subinterface-number* {**multipoint | point-to-point**}]

or

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	**interface atm** *slot*/**0**[**.***subinterface-number* {**multipoint** | **point-to-point**}] or **interface atm** *slot*/*port-adapter*/**0**[**.***subinterface-number* {**multipoint** | **point-to-point**}] or **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.[1] 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.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM VC configuration mode and returns to interface configuration mode.

1. 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.
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 VC Enhancements

This section provides the following configuration examples:

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

The following sections provide references related to the ATM SNMP Trap and OAM Enhancements feature.

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

Feature Information for Configuring ATM SNMP Trap and OAM VC Enhancements

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 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: • Information About Configuring ATM SNMP Trap and VC OAM Enhancements, page 2 • How to Configure ATM SNMP Trap and VC OAM Enhancements, page 5 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.
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 sections provide information about this feature: • ATM OAM AIS-RDI Monitoring, page 3 • Enabling OAM AIS-RDI Monitoring, page 8 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.

IMA Dynamic Bandwidth

First Published: March 17, 2005
Last Updated: October 02, 2009

The IMA Dynamic Bandwidth feature introduces the ability to configure Cisco IOS software to automatically manage changes in the total bandwidth of an Asynchronous Transfer Mode (ATM) interface configured with an Inverse Multiplexing over ATM (IMA) group. This feature eliminates manual intervention required when an individual link goes up or down, and allows the available bandwidth to be used effectively.

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 IMA Dynamic Bandwidth" section on page 8.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for IMA Dynamic Bandwidth

This feature requires the following:

- An ATM interface must be configured for IMA operation.
- An IMA group interface must be configured.

Restrictions for IMA Dynamic Bandwidth

The restrictions are as follows:

- This feature is supported only for ATM permanent virtual circuits (PVCs). Switched virtual circuits (SVCs) are not supported.
- This feature is supported only for the unspecified bit rate (UBR), available bit rate (ABR), and variable bit rate nonreal-time (VBR-NRT) quality of service (QoS) classes.
- The algorithm used to implement this feature is applied only when dynamic changes to an IMA group interface occur. It is not applied at VC creation on router bootup.
- Incorrect QoS parameters may be applied to PVCs if the IMA Dynamic Bandwidth feature is disabled after a change in total bandwidth, and then enabled again after another change in total bandwidth.

Information About IMA Dynamic Bandwidth

To configure the IMA Dynamic Bandwidth feature, you should understand the following concepts:

- IMA Groups, page 2
- Dynamic Changes in Bandwidth Availability, page 2
- How the IMA Dynamic Bandwidth Feature Works, page 3

IMA Groups

IMA provides the capability to send and receive a single high-speed ATM data stream over multiple slower-speed physical links. The originating stream of ATM cells is divided so that complete ATM cells are sent in round-robin order across the set of ATM links.

IMA requires the configuration of a logical ATM interface. The logical ATM interface is called an IMA group, and consists of multiple physical ATM links. VCs are configured under the IMA group interface, and can send data over any or all of the physical ATM links in the group.

Dynamic Changes in Bandwidth Availability

When multiple T1 or E1 lines are grouped into an IMA group, the total available bandwidth is the sum of the bandwidth of each line. If one or more of the lines goes down, the total bandwidth available on the IMA group interface is reduced. If a line then come back up, the total available bandwidth increases. These dynamic changes in available total bandwidth impact the bandwidth that is available for any VC configured on the IMA group interface.

How the IMA Dynamic Bandwidth Feature Works

When the total available bandwidth on an IMA group interface changes, all of the PVCs configured on that interface are re-created.

If necessary and applicable for a particular PVC based on its QoS class, new values are applied for the following parameters when PVCs are re-created:

- PCR—peak cell rate
- MCR—minimum cell rate
- SCR—sustainable cell rate

The following steps are performed by the Cisco IOS software to determine what value should be assigned to a parameter when a PVC is re-created in response to a change in total available bandwidth:

- A value is calculated for the parameter. The calculation takes into account the configured value for the parameter, the active value for the parameter (if it is different from the configured value), and the change in total available bandwidth.
- The calculated value is compared to the configured value of the parameter and to the maximum available cell rate, and a new value is determined. The new value is applied when the PVC is re-created.

Note The configured value of a parameters is not overwritten in the configuration file by any new value that is applied in response to dynamic bandwidth changes.

The following sections describe how the new parameter values are determined when a PVC is re-created for supported QoS classes:

- UBR PVCs
- ABR PVCs
- VBR-NRT PVCs

UBR PVCs

When the total available bandwidth changes, PVCs configured with UBR QoS are re-created as follows:

- If the PCR configuration is set to the default, the PVC is re-created with a PCR value equal to the maximum available rate.
- If the configured PCR value is less than the calculated PCR value, the PVC is re-created with the configured PCR value.
- If the configured PCR value is greater than the calculated PCR value, the PVC is re-created with a new PCR value. The new PCR value will be the lower of the following values:
  - The calculated PCR value
  - The maximum available cell rate

ABR PVCs

When the total available bandwidth changes, PVCs configured with ABR QoS are re-created as follows:

- If the configured PCR value is less than the calculated PCR value, the PVC is re-created with the configured PCR value.
- If the configured PCR value is greater than the calculated PCR value, the PVC is re-created with a new PCR value. The new PCR value will be the lesser of the following values:

  - The calculated PCR value
  - The maximum available cell rate
- If the configured MCR value is less than the calculated MCR value, the PVC is re-created with the configured MCR value.
- If the configured MCR value is greater than the calculated MCR value, the PVC is re-created with the calculated MCR value.

VBR-NRT PVCs

If the total available bandwidth decreases or increases, VBR-NRT PVCs will be re-created as follows:

- If the configured PCR value is less than the calculated PCR value, the PVC is re-created with the configured PCR value.
- If the configured PCR value is greater than the calculated PCR value, the PVC is re-created with a new PCR value. The new PCR value will be the lesser of the following values:
  - The calculated PCR value
  - The maximum available cell rate
- If the configured SCR value is less than the calculated SCR value, the PVC is re-created with the configured SCR value.

If the configured SCR value is greater than the calculated SCR value, the PVC is re-created with a the calculated SCR value.

How to Enable IMA Dynamic Bandwidth

This section contains the following:

- Enabling IMA Dynamic Bandwidth, page 4

Enabling IMA Dynamic Bandwidth

The IMA Dynamic Bandwidth feature allows Cisco IOS software to make dynamic adjustments to VC bandwidth in response to changes in the overall IMA interface bandwidth.

Perform this task to enable the IMA Dynamic Bandwidth feature.

Note Incorrect QoS parameters may be applied to PVCs if the IMA Dynamic Bandwidth feature is disabled after a change in total bandwidth, and then reenabled after another change in total bandwidth.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot*/**ima** *group-number*
4. **atm bandwidth dynamic**

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*/**ima** *group-number* **Example:** `Router(config)# interface atm 3/ima 1`	Configures an IMA group and enters interface configuration mode.
Step 4	**atm bandwidth dynamic** **Example:** `Router(config-if)# atm bandwidth dynamic`	Enables the automatic management of changes in the total bandwidth of an ATM interface configured with an IMA group.

Configuration Examples for IMA Dynamic Bandwidth

This section contains the following configuration example:

- Enabling the IMA Dynamic Bandwidth Feature: Example, page 5

Enabling the IMA Dynamic Bandwidth Feature: Example

The following example creates IMA group 1, enables automatic bandwidth management, and assigns a physical ATM interface to the IMA group:

```
interface atm3/ima 1
 atm bandwidth dynamic
!
interface atm0/1
 ima-group 1
```

Additional References

The following sections provide references related to the IMA Dynamic Bandwidth feature.

Related Documents

Related Topic	Document Title
Configuring IMA	Configuring ATM
ATM Commands	ATM Commands

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/techsupport

Feature Information for IMA Dynamic Bandwidth

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for IMA Dynamic Bandwidth

Feature Name	Releases	Feature Information
IMA Dynamic Bandwidth	12.0(30)S1	The IMA Dynamic Bandwidth feature provides the ability to configure Cisco IOS software to automatically adjust PVC bandwidth in response to changes in the total available IMA group interface bandwidth. In 12.0(30)S1, this feature was introduced on the Cisco 12000 and 4500 series router. The following sections provide information about this feature: • Information About IMA Dynamic Bandwidth, page 2 • How to Enable IMA Dynamic Bandwidth, page 4 The following commands were introduced or modified: **atm bandwidth dynamic**.

Define Interface Policy-Map AV Pairs AAA

Last Updated: October 2, 2009

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco Remote Authentication Dial-In User Service (RADIUS) vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level.

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" section on page 18.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Define Interface Policy-Map AV Pairs AAA

- Authentication, Authorization, and Accounting (AAA) must be enabled and already set up to use RADIUS.
- Configuring a service policy on the ATM subinterface requires enabling Dynamic Bandwidth Selection (DBS) on the VC.

Restrictions for Define Interface Policy-Map AV Pairs AAA

For the Cisco 7000 Series Routers

- Only the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters are supported for this feature.

For the Cisco 10000 Series Routers

- You cannot configure a service policy on a VC and on a session at the same time.
- All ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, are supported for this feature.

Information About Define Interface Policy-Map AV Pairs AAA

The following concept is described in this section:

- Dynamically Applying and Modifying a Policy Map

Dynamically Applying and Modifying a Policy Map

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco VSAs that allow you to dynamically apply a policy map and modify a policy map applied to a session, without session reauthentication, at the ATM VC level using RADIUS. The purpose of the Cisco VSA (attribute 26) is to communicate vendor-specific information between the network access server (NAS) and the RADIUS server. The Cisco VSA encapsulates vendor-specific attributes that allow vendors such as Cisco to support their own extended attributes.

The Define Interface Policy-Map AV Pairs AAA feature allows the two new Cisco VSAs to be installed on an ATM VC after a PPPoA or PPPoEoA session establishment. Using RADIUS, this feature allows a policy map to be applied (“pulled”) and then modified by specific events (“pushed” by the policy server) while that session remains active.

Previously, a policy map could only be configured on a VC or ATM point-to-point subinterface by using the modular QoS CLI (MQC) or manually with the virtual template. Also previously, a service policy on a VC could be modified in the session but that session was dropped and reauthenticated. Currently for a PPPoA or PPPoEoA session, the pull part of the feature uses RADIUS to dynamically apply policy maps on an ATM VC and eliminates the need to statically configure a policy map on each VC. After a policy map is applied directly on the interface, certain events can signal the policy server to push a policy map onto a specific VC without the need for session reauthentication.

Note Configuring a service policy on the ATM subinterface still requires MQC configuration.

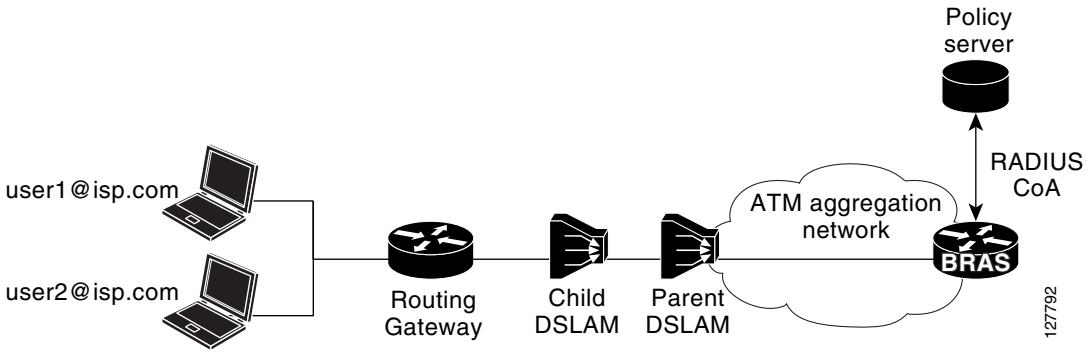
Two new Cisco AV pairs for service policy are set up in the user file on the RADIUS server. When the router requests the policy map name, the policy map name in the user file is pulled to the VC on the router when the PPPoA or PPPoEoA session is established. The Cisco AV pairs identify a "service policy-output" and "service policy-input" to identify QoS policies configured on the router from a RADIUS server. The Cisco AV pairs apply the appropriate policy map directly on the interface. Service policies are only applied at this time when the subscriber first authenticates the VC.

The "push" functionality of the feature allows you to modify an existing QoS profile (a policy map) applied to a session while that session remains active, thus allowing QoS policies to be applied as required without session reauthentication disruption. Specific events, including time-of-day, byte count, and user request, can signal the policy server to push a policy map onto a specific VC.

The policy server has the ability to send a Change of Authorization (CoA), which is the ability to change authorization of active sessions on the fly. The push functionality requires that CoA is enabled on the AAA server. One of the session attributes CoA pushes is the policy map, in an input and output direction.

Figure 1 shows that a CoA request is sent from the policy server to a broadband rate access server (BRAS), which causes a policy map change on PPPoA sessions set up between the BRAS and the routing gateway (RG).

Figure 1 Change of Authorization—Policy Map Change on PPPoA Sessions



For more information on configuring CoA support on the server, see the "Enabling ISA to Interact with External Policy Servers" chapter in the *Cisco ISA RADIUS COA Interface Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122sba27/isa/isa_cg/is_aaa.htm

For clarification, a policy map defines QoS actions and rules and associates these to a class map. In a policy map, you can define QoS actions for such things as policing and class-based weighted fair queuing (CBWFQ). After a policy map is configured on the router with the **policy-map** command, using the **service-policy** command attaches the configured policy map to a VC interface and specifies the direction (inbound or outbound) that the policy should be applied.

When a service policy is configured on the VC (or ATM point-to-point subinterface), the service policy is applied to all sessions that use that VC. This allows class-based weighted fair queuing (CBWFQ) to be applied to sessions.

Note For the Cisco 7200 series routers, you can configure a service policy on a VC and on a session at the same time. On the Cisco 10000 series routers, you must either configure a service policy on a VC or on a session, but not both at the same time.

Note The Cisco 7200 series routers and Cisco 7301 router only support the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters for this feature. The Cisco 10000 series routers support all ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, for this feature.

New Cisco VSAs

To support the Define Interface Policy-Map AV Pairs AAA feature, the following two new Cisco AV pairs for policy map are defined at the ATM VC level:

- Cisco VSA attribute is vc-qos-policy-in
- Cisco VSA attribute is vc-qos-policy-out

They are formatted as:

- cisco-avpair = “atm:vc-qos-policy-in=<*in policy name*>”
- cisco-avpair = “atm:vc-qos-policy-out=<*out policy name*>”

To further support the Define Interface Policy-Map AV Pairs AAA feature, two existing Cisco Generic RADIUS VSAs will replace and deprecate two others that do not correctly follow the Cisco VSA naming guidelines.

The two replacement VSAs are:

- cisco-avpair = “ip:sub-qos-policy-in=<*in policy name*>”
- cisco-avpair = “ip:sub-qos-policy-out=<*out policy name*>”

The replacement VSAs replace the following existing VSAs:

- cisco-avpair = “ip:sub-policy-In=<*in policy name*>”
- cisco-avpair = “ip:sub-policy-Out=<*out policy name*>”

We recommend using the new VSAs. However, the replaced attributes are currently still supported.

Policy Map Troubleshooting Scenarios

- If a policy map is already configured on the ATM VC, the policy map pulled from the RADIUS server has higher precedence. This means that a **show policy-map** command shows the policy map pulled from the RADIUS server.
- After a policy map is successfully pulled on the VC, any configuration or unconfiguration after that using the **[no] service-policy input/output** *name* command does not affect the policy map used by the VC. Issuing a **show policy-map** command displays the pulled policy map. Issuing a **show run** command displays the current user configuration on the router.
- To remove the dynamic policy that is pulled from the RADIUS server, use the **no dbs enable** command or clear the PPPoA or PPPoEoA session associated with the VC.

- You should push both the input and output policy map together on the VC. If you push only one policy in one direction (for example, the input direction), then the output direction by default is a null policy push. The result is that on the VC, the input policy map is the policy pushed by the change of authorization (CoA). The output policy map is whatever policy was configured locally on the VC. If no output policy map was configured on the VC, there is no output policy map.

Benefits of Define Interface Policy-Map AV Pairs AAA

- The ability to apply QoS policies transparently as required without the disruption of session reauthentication provides a high degree of flexibility, smaller configuration files, and more efficient usage of queuing resources. This ability eliminated the need to pre-provision subscribers.
- The ability to modify the applied policy map as needed without session disruption (session dropped and reauthenticated) is an advantage to service providers.
- Nondisruptive support for special event triggers is essential to support new dynamic bandwidth services such as pre-paid and turbo button services.
- The QoS policy map is used to define the subscriber user experience for broadband service and can facilitate delivery of higher value services such as VoIP and video.

How to Define Interface Policy-Map AV Pairs AAA

This section contains the following tasks:

- Configuring AV Pairs, Dynamic Authorization, and the Policy Map, page 5
- Verifying Define Interface Policy-Map AV Pairs AAA, page 9

Configuring AV Pairs, Dynamic Authorization, and the Policy Map

To configure the Define Interface Policy-Map AV Pairs AAA feature, follow the steps below on both the router and the RADIUS server.

Prerequisites

- Authentication, Authorization, and Accounting (AAA) must be enabled and already set up to use RADIUS.
- A PPPoEoA or PPPoA session is established.
- The change of authorization (CoA) functionality is enabled—required for the push functionality.
- The **dbs enable** CLI is configured on the VC.
- The policy map is configured on the router.

SUMMARY STEPS

On the RADIUS server, configure the new Cisco AV pair attributes in the user file:

```
atm:vc-qos-policy-in=<in policy name>
atm:vc-qos-policy-out=<out policy name>
```

On the local AAA server, configure dynamic authorization that supports Change of Authorization.

1. **aaa server radius dynamic-author**
   client {*ip_addr* | *name*} [**vrf** {*vrfname*}] [**server-key** {*string*}]

On the router:

1. **enable**
2. **configure terminal**
3. **interface atm** [*module/slot/port.subinterface*] **point-to-point**
4. **pvc** *vpi/vci*
5. **dbs enable**
6. **exit**
7. **policy-map** *policy-map-name*
8. **end**

DETAILED STEPS—RADIUS Server

	Command or Action	Purpose
Step 1	`atm:vc-qos-policy-in=<in policy name>` **`atm:vc-qos-policy-out=<out policy name>`** On the RADIUS server, configure in the user file: `userid  Password ="cisco"` `  Service-Type = Framed,` `  Framed-Protocol = PPP,` `  cisco-avpair = "atm:vc-qos-policy-out=dyn_out",` `  cisco-avpair = "atm:vc-qos-policy-in=test_vc"`	Enters the two new Cisco AV pairs for service policy on the RADIUS server in the user file. When the router requests the policy name, this information in the user file is "pulled." A RADIUS user file contains an entry for each user that the RADIUS server will authenticate. Each entry, which is also referred to as a *user profile*, establishes an attribute the user can access. When looking at a user file, the data to the left of the equal sign (=) is an attribute defined in the dictionary file, and the data to the right of the equal sign is the configuration data. In this example, you have configured a service policy that attaches a policy map to the ATM VC interface and specifies the direction (inbound for data packets traveling into the interface or outbound for data packets leaving the interface). The policy map applied in the outbound direction is dyn_out and the inbound policy map is test_vc.

DETAILED STEPS—AAA Server

	Command or Action	Purpose
Step 1	**aaa server radius dynamic-author** **client** {*ip_addr* | *name*} [**vrf** {*vrfname*}] [**server-key** {*string*}] **server-key** [**0** | **7**] {*string*} **port** {*port-num*} **auth-type** {**any** | **all** | **session-key**} **ignore session-key** **ignore server-key** On the AAA server, the following is an example configuration: `aaa server radius dynamic-author` `client 192.168.0.5 vrf coa server-key cisco1` `client 192.168.1.5 vrf coa server-key cisco2`	Sets up the local AAA server for dynamic authorization service, which must be enabled to support the CoA functionality that can push the policy map in an input and output direction. • To enable CoA to work, you must configure the **aaa server radius dynamic-author** command, and **client** and **server-key** keywords. • You can configure the server-key by using the **client** [**server-key** {*string*}] keywords to configure at the "client" level, or use the **server-key** {*string*} keyword to configure at the "global" level. • Using the **server-key** {*string*} keyword in submode is global because it allows all the clients already configured using **client** [**server-key** {*string*}] to use the server-key as specified in the **server-key** {*string*} keyword. However, note that configuring at the client level overrides the global level. For security purposes, we recommend configuring each client and using different server-keys for each client. The example configuration enables change of authorization with the **dynamic-author** command that also configures two client routers with different server-keys (cisco1 and cisco2). The **port**, **auth-type**, **ignore session-key**, and **ignore server-key** keywords are optional.

DETAILED STEPS—Router

	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** [*module/slot/port.subinterface*] **point-to-point** **Example:** `Router(config)# interface ATM4/0 point-to-point`	Specifies the interface, for example ATM4/0, and the encapsulation type on an ATM PVC and enters subinterface mode.
Step 4	**pvc** *vpi/vci* **Example:** `Router(config-if)# pvc 1/101`	Creates or assigns a name to an ATM permanent virtual circuit (PVC) in subinterface configuration mode. • The **pvc** command creates a PVC and attaches it to the virtual path identifier (VPI) and virtual channel identifier (VCI) specified. • Enters ATM virtual circuit configuration mode. • The example specifies VPI 1 and VCI 101 for this PVC. For more information on the command, refer to the *Cisco IOS Wide-Area Networking Command Reference, Release 12.3T,* Commands M through R.
Step 5	**dbs enable** **Example:** `Router(config-if-atm-vc)# dbs enable`	Enables Dynamic Bandwidth Selection (DBS) in ATM VC configuration mode. Enabling this command allows the ATM shaping parameters to be retrieved from the RADIUS user profile. • For more information on the command, refer to the *Cisco IOS Wide-Area Networking Command Reference, Release 12.3T,* Commands D through E. **Note** The **no dbs enable** command re-creates the VC and removes the dynamic policy that is pulled from the RADIUS server. Consequently, any configured modular QoS CLI (MQC) policy map on the PVC will be installed on the VC. Do not issue the **no dbs enable** command when the VC is active.
Step 6	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM VC configuration mode and returns to subinterface configuration mode. • Repeat this step one more time to exit subinterface configuration mode and return to global configuration mode.

	Command or Action	Purpose
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map voice`	Creates a policy map on the router. • In the example, a policy map named voice is created.
Step 8	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Define Interface Policy-Map AV Pairs AAA

Perform this optional task to verify the configuration of the Define Interface Policy-Map AV Pairs AAA feature.

SUMMARY STEPS

1. **show policy-map**
2. **show running-config**
3. **show running-config**

DETAILED STEPS

Step 1 show policy-map interface

The **show policy-map interface** command shows the policy map voice attached to the ATM VC:

```
Router# show policy-map interface atm 4/0
ATM4/0: VC 1/101 -

 Service-policy input: voice

   Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Step 2 show running-config

The following example displays the running configuration on the router showing the AAA setup; policy map configuration; ATM VC, PPPoA, and DBS-enabled CLI configuration; Virtual-Template configuration; and RADIUS server configuration:

```
Router# show running-config

.
.
.

aaa new-model
!
aaa user profile TEST
!
```

```
aaa authentication ppp default group radius
aaa authorization network default group radius
!

aaa session-id common
ip subnet-zero

.
.
.

policy-map voice
class Class-Default
fair-queue

.
.
.

!
interface ATM4/0.1 point-to-point
 pvc 1/101
  dbs enable
  encapsulation aal5mux ppp Virtual-Template1
 !

.
.
.
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp authentication chap
!

.
.
.

!
radius-server host 172.19.197.225 auth-port 1890 acct-port 1891
radius-server timeout 15
radius-server key 7 060506324F41
radius-server vsa send accounting
radius-server vsa send authentication
!

.
.
.

!
!
end
```

Step 3 show running-config

The following example displays the PPPoA client configuration:

```
.
.
.
```

```
!
interface ATM4/0.1 point-to-point
 pvc 1/101
  encapsulation aal5mux ppp Virtual-Template1
 !
!
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp chap hostname userid
 ppp chap password 7 030752180500
!

.
.
.
```

Configuration Examples for Define Interface Policy-Map AV Pairs AAA

This section contains the following examples:

Service-Policy Map Already Configured: Example

The following example shows the existing MQC used to attach policy maps voice and outname under PVC 4/103. Using the **show policy-map interface** command shows that MQC-configured policy maps voice and outname are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
  service-policy input voice
  service-policy output outname
 !
Router# show policy-map interface atm 4/0.3
 ATM4/0.3: VC 4/103 -

  Service-policy input: voice

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps

  Service-policy output: outname

    Class-map: class-default (match-any)
```

```
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
Router#
```

The following example shows MQC used to establish a PPPoEoA session, which causes the policy maps (test_vc and dyn_out) set up on the RADIUS server to be downloaded or "pulled" to the VC. The policy maps downloaded from the RADIUS server have higher precedence than the MQC service-policy maps (voice and outname) configured on the PVC. Using the **show policy-map interface** command shows that the pulled policy maps are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
  dbs enable
  encapsulation aal5autoppp Virtual-Template1
  service-policy input voice
  service-policy output outname
 !
end

Router# show policy-map interface atm 4/0.3
 ATM4/0.3: VC 4/103 -

  Service-policy input: test_vc

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps

  Service-policy output: dyn_out

    Class-map: class-default (match-any)
      5 packets, 370 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        5 packets, 370 bytes
        5 minute rate 0 bps
Router#

PPPoE Session Information
Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st
      2      2  0010.1436.bc70  ATM4/0.3                 1  Vi3.1      PTA
                0010.1436.b070  VC:  4/103                  UP
Router#
```

Service-Policy Map Pulled: Example

The following example shows a policy named voice configured for input service policy on the RADIUS server. The router is already configured for PPPoA and AAA. The PPPoA session pulls the service policy name from the RADIUS server.

The **show policy-map interface** command displays the input service policy named voice attached to the ATM interface:

```
Router# show policy-map interface atm 4/0.1
ATM4/0: VC 1/101 -

 Service-policy input: voice

   Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Using the **show run interface** command displays the currently running configuration, but not the pulled service policy:

```
Router# show run interface atm 4/0.1

Building configuration...

Current configuration : 107 bytes
!
interface ATM 4/0.1
    pvc 1/101
         dbs enable
         encapsulation aal5mux ppp Virtual-Template 1
    !
!
end
```

Service-Policy Map Pushed: Example

This configuration example has five parts that show that PPPoA sessions are established between a broadband remote access server (BRAS) and a routing gateway (RG), the change of authorization (CoA push request) that passes between a policy server and the BRAS, and how the pulled policy maps are replaced by pushed policy maps after the CoA request.

The five parts are: BRAS PPPoA configuration, RG PPPoA configuration, session information on BRAS prior to a push, debug on BRAS after receiving the CoA request, and session information on BRAS after a CoA push request has taken place.

The following example shows the current PPPoA configuration on BRAS:

```
aaa new-model
 !
 aaa authentication ppp default group radius
 aaa authorization network default group radius
 !
 aaa server radius dynamic-author
  client <address> server-key <key>
 !
 aaa session-id common
 !
 ip routing
 !
 policy-map DefaultIn
   class class-default
   set ip precedence 0
 policy-map DefaultOut
   class class-default
   set ip precedence 0
 !
```

```
policy-map PullMapIn
  class class-default
  set ip precedence 0
policy-map PullMapOut
  class class-default
  set ip precedence 0
!
policy-map 7up
  class class-default
    fair-queue
policy-map Sprite
  class class-default
    bandwidth 1000
!
policy-map PushMapIn
  class class-default
  set ip precedence 0
policy-map PushMapOut
  class class-default
  set ip precedence 0
!
!
vc-class atm xyz
  protocol ppp Virtual-Template1
  encapsulation aal5snap
!
interface Loopback0
 ip address 12.1.1.2 255.255.255.0
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
 no atm enable-ilmi-trap
 no clns route-cache
 no shutdown
!
interface ATM4/0.1 point-to-point
 no atm enable-ilmi-trap
 pvc 0/101
  class-vc xyz
  vbr-nrt 400 300 50
  dbs enable
  service-policy in DefaultIn
  service-policy out DefaultOut
 !
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ppp authentication chap
!
radius-server host <address> auth-port <port> acct-port <port>
radius-server key <key>
radius-server vsa send authentication
```

The following example shows the PPPoA configuration set up on the RG:

```
aaa new-model
 !
 aaa session-id common
 !
 ip routing
 !
 interface Loopback0
```

```
 ip address 12.1.1.1 255.255.255.0
!
interface ATM2/0/0
 no ip address
 no atm ilmi-keepalive
 no atm enable-ilmi-trap
 no clns route-cache
 no shutdown
!
interface ATM2/0/0.1 point-to-point
 pvc 0/101
  protocol ppp Virtual-Template1
 !
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no peer default ip address
 ppp chap hostname InOut
 ppp chap password 0 <password>
```

The following example uses the **show subscriber session all** command to display session information on BRAS prior to policy maps being pushed. PullMapIn and PullMapOut are the profiles pulled from the AAA server. The CoA request pushes the BRAS to change its input policy map (PullMapIn) and output policy map (PullMapOut) to PushMapIn and PushMapOut respectively.

```
Router# show subscriber session all

Current Subscriber Information:Total sessions 1
------------------------------------------------
Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:32, Last Changed:00:00:12
AAA unique ID:55
Interface:Virtual-Access1.1

Policy information:
  Context 6531F6AC:Handle C700008A
  Authentication status:authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    service-type         2 [Framed]
    ssg-account-info     "S12.1.1.1"
    vc-qos-policy-in     "PullMapIn"
    vc-qos-policy-out    "PullMapOut"
  Prepaid context:not present


Configuration sources associated with this session:
Interface:Virtual-Template1, Active Time = 00:00:32
```

The following example displays the output of the **debug aaa coa** and **debug pppatm event** commands to show that the input policy map, PushMapIn, and output policy map, PushMapOut, have been applied or pushed on the BRAS after the BRAS received the CoA push request from the policy server:

```
2d20h:RADIUS:COA  received from id 41 10.0.56.145:1700, CoA Request, len 122
2d20h:COA:10.0.56.145 request queued
2d20h: ++++++ CoA Attribute List ++++++
2d20h:6523AE20 0 00000001 service-type(276) 4 Framed
2d20h:6523AF4C 0 00000009 ssg-account-info(392) 9 S12.1.1.1
2d20h:6523AF5C 0 00000009 ssg-command-code(394) 1 17
```

```
2d20h:6523AF6C 0 00000009 vc-qos-policy-in(342) 7 PushMapIn
2d20h:6523AF7C 0 00000009 vc-qos-policy-out(343) 4 PushMapOut
2d20h:
2d20h: PPPATM:Received VALID vc policy PushMapIn
2d20h: PPPATM:Received VALID vc policy PushMapOut
2d20h:PPPATM:ATM4/0.1 0/101 [54], Event = SSS Msg Received = 5
2d20h:Service policy input PushMapIn policy output PushMapOut applied on 0/101
2d20h: PPPATM:Applied VALID vc policy PushMapIn and PushMapOut
2d20h:RADIUS(00000000):sending
2d20h:RADIUS(00000000):Send CoA Ack Response to 10.0.56.145:1700 id 41, len 20
2d20h:RADIUS: authenticator 04 D5 05 E2 FE A3 A6 E5 - B2 07 C0 A1 53 89 E0 FF
```

The following example uses the **show subscriber session all** command to display session information on the BRAS after the BRAS received the CoA push request from the policy server. The policy information shows that PushMapIn and PushMapOut are the current policy maps on the BRAS that were pushed by the CoA request:

```
Router# show subscriber session all
Current Subscriber Information:Total sessions 1
------------------------------------------------
Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:44, Last Changed:00:00:22
AAA unique ID:55
Interface:Virtual-Access1.1

Policy information:
  Context 6531F6AC:Handle C700008A
  Authentication status:authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    service-type         2 [Framed]
    ssg-account-info     "S12.1.1.1"
    vc-qos-policy-in     "PushMapIn"
    vc-qos-policy-out    "PushMapOut"
  Prepaid context:not present


Configuration sources associated with this session:
Interface:Virtual-Template1, Active Time = 00:00:44
```

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).	"Enabling ISA to Interact with External Policy Servers" chapter in the *Cisco ISA RADIUS COA Interface Guide*. 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
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 Define Interface Policy-Map AV Pairs AAA

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Define Interface Policy-Map AV Pairs AAA

Feature Name	Releases	Feature Information
Define Interface Policy-Map AV Paris AAA:Pulled	12.3(7)XI2	This feature was integrated into Cisco IOS Release 12.3(7)XI2 and introduced for the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The "pulled" functionality was implemented. The following sections provide information about this feature: • Service-Policy Map Pulled: Example, page 12 No new or modified commands.
Define Interface Policy-Map AV Paris AAA:Pushed	12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB. Support for the "pushed" functionality was added on the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The following sections provide information about this feature: Service-Policy Map Pushed: Example, page 13 No new or modified commands.