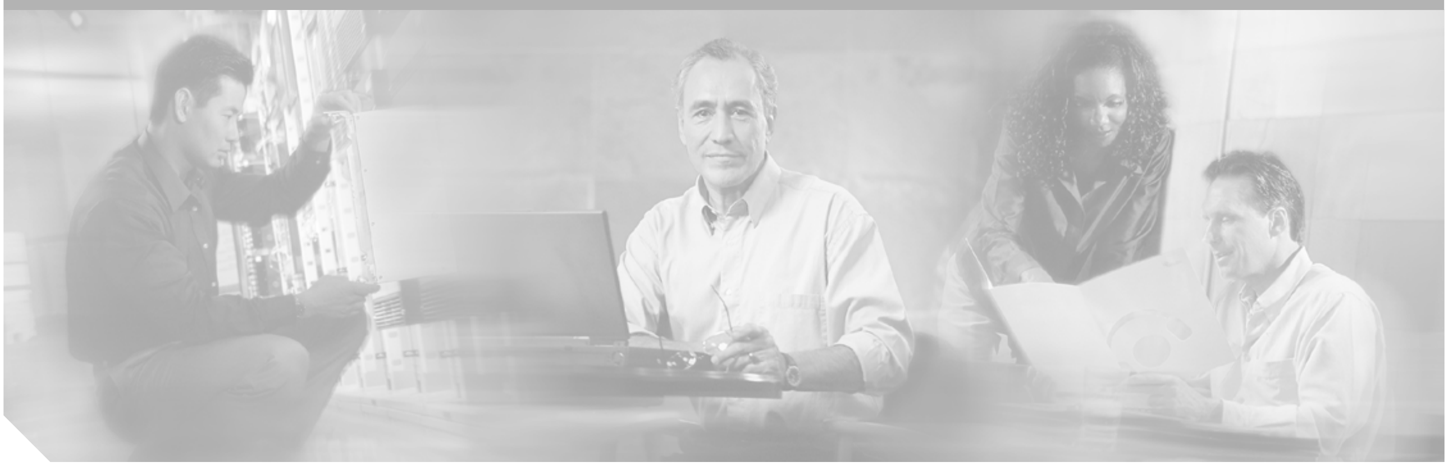


Cisco IOS Asynchronous Transfer Mode Configuration Guide

Release 12.4

Corporate 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: 408 526-4100

Customer Order Number: DOC-7817500=
Text Part Number: 78-17500-01


CONTENTS

MPOA Overview

About Cisco IOS Software Documentation for Release 12.4

This chapter describes the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation, technical assistance, and additional publications and information from Cisco Systems. It contains the following sections:

Documentation Objectives

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

Audience

The Cisco IOS software documentation set is intended primarily 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 software commands necessary to perform particular tasks. The Cisco IOS software 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 software release.

Documentation Organization for Cisco IOS Release 12.4

The Cisco IOS Release 12.4 documentation set consists of the configuration guide and command reference pairs listed in Table 1 and the supporting documents listed in Table 2. The configuration guides and command references are organized by technology. For the configuration guides:

- Some technology documentation, such as that for DHCP, contains features introduced in Releases 12.2T and 12.3T and, in some cases, Release 12.2S. To assist you in finding a particular feature, a roadmap document is provided.
- Other technology documentation, such as that for OSPF, consists of a chapter and accompanying Release 12.2T and 12.3T feature documents.

Note In some cases, information contained in Release 12.2T and 12.3T feature documents augments or supersedes content in the accompanying documentation. Therefore it is important to review all feature documents for a particular technology.

Table 1 lists the Cisco IOS Release 12.4 configuration guides and command references.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Description
IP	
Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 *Cisco IOS IP Addressing Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP addressing and services, including Network Address Translation (NAT), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Application Services Configuration Guide, Release 12.4 *Cisco IOS IP Application Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP application services, including IP access lists, Web Cache Communication Protocol (WCCP), Gateway Load Balancing Protocol (GLBP), Server Load Balancing (SLB), Hot Standby Router Protocol (HSRP), and Virtual Router Redundancy Protocol (VRRP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Mobility Configuration Guide, Release 12.4 *Cisco IOS IP Mobility Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Mobile IP and Cisco Mobile Networks. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Multicast Configuration Guide, Release 12.4 *Cisco IOS IP Multicast Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP multicast, including Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Source Discovery Protocol (MSDP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4 *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF). The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS IP Switching Configuration Guide, Release 12.4 *Cisco IOS IP Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP switching features, including Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IPv6 Configuration Guide, Release 12.4 *Cisco IOS IPv6 Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP version 6 (IPv6), including IPv6 broadband access, IPv6 data-link layer, IPv6 multicast routing, IPv6 quality of service (QoS), IPv6 routing, IPv6 services and management, and IPv6 tunnel services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Optimized Edge Routing Configuration Guide, Release 12.4 *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Optimized Edge Routing (OER) features, including OER prefix learning, OER prefix monitoring, OER operational modes, and OER policy configuration. The command reference provides detailed information about the commands used in the configuration guide.
Security and VPN	
Cisco IOS Security Configuration Guide, Release 12.4 *Cisco IOS Security Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring various aspects of security, including terminal access security, network access security, accounting, traffic filters, router access, and network data encryption with router authentication. The command reference provides detailed information about the commands used in the configuration guide.
QoS	
Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4 *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring quality of service (QoS) features, including traffic classification and marking, traffic policing and shaping, congestion management, congestion avoidance, and signaling. The command reference provides detailed information about the commands used in the configuration guide.
LAN Switching	
Cisco IOS LAN Switching Configuration Guide, Release 12.4 *Cisco IOS LAN Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to local-area network (LAN) switching features, including configuring routing between virtual LANs (VLANs) using Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, and IEEE 802.1Q encapsulation. The command reference provides detailed information about the commands used in the configuration guide.
Multiprotocol Label Switching (MPLS)	
Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4 *Cisco IOS Multiprotocol Label Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Multiprotocol Label Switching (MPLS), including MPLS Label Distribution Protocol, MPLS traffic engineering, and MPLS Virtual Private Networks (VPNs). The command reference provides detailed information about the commands used in the configuration guide.
Network Management	
Cisco IOS IP SLAs Configuration Guide, Release 12.4 *Cisco IOS IP SLAs Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the Cisco IOS IP Service Level Assurances (IP SLAs) feature. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS NetFlow Configuration Guide, Release 12.4 *Cisco IOS NetFlow Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to NetFlow features, including configuring NetFlow to analyze network traffic data, configuring NetFlow aggregation caches and export features, and configuring Simple Network Management Protocol (SNMP) and NetFlow MIB features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Network Management Configuration Guide, Release 12.4 *Cisco IOS Network Management Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to network management features, including performing basic system management, performing troubleshooting and fault management, configuring Cisco Discovery Protocol, configuring Cisco Networking Services (CNS), configuring DistributedDirector, and configuring Simple Network Management Protocol (SNMP). The command reference provides detailed information about the commands used in the configuration guide.
Voice	
Cisco IOS Voice Configuration Library, Release 12.4 *Cisco IOS Voice Command Reference*, Release 12.4	The configuration library is a task-oriented collection of configuration guides, application guides, a troubleshooting guide, feature documents, a library preface, a voice glossary, and more. It also covers Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. In addition, the library includes documentation for IP telephony applications. The command reference provides detailed information about the commands used in the configuration library.
Wireless/Mobility	
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring a Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunication System (UMTS) network. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Home Agent Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Home Agent Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Mobile Wireless Home Agent, which is an anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Packet Data Serving Node (PDSN), a wireless gateway between the mobile infrastructure and standard IP networks that enables packet data services in a Code Division Multiple Access (CDMA) environment. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring Cisco IOS Radio Access Network products. The command reference provides detailed information about the commands used in the configuration guide.
Long Reach Ethernet (LRE) and Digital Subscriber Line (xDSL)	
Cisco IOS Broadband and DSL Configuration Guide, Release 12.4 *Cisco IOS Broadband and DSL Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring broadband access aggregation and digital subscriber line features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Service Selection Gateway Configuration Guide, Release 12.4 *Cisco IOS Service Selection Gateway Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Service Selection Gateway (SSG) features, including subscriber authentication, service access, and accounting. The command reference provides detailed information about the commands used in the configuration guide.
Dial—Access	
Cisco IOS Dial Technologies Configuration Guide, Release 12.4 *Cisco IOS Dial Technologies Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring lines, modems, and ISDN services. This guide also contains information about configuring dialup solutions, including solutions for remote sites dialing in to a central office, Internet service providers (ISPs), ISP customers at home offices, enterprise WAN system administrators implementing dial-on-demand routing, and other corporate environments. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS VPDN Configuration Guide, Release 12.4 *Cisco IOS VPDN Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Virtual Private Dialup Networks (VPDNs), including information about Layer 2 tunneling protocols, client-initiated VPDN tunneling, NAS-initiated VPDN tunneling, and multihop VPDN. The command reference provides detailed information about the commands used in the configuration guide.
Asynchronous Transfer Mode (ATM)	
Cisco IOS Asynchronous Transfer Mode Configuration Guide, Release 12.4 *Cisco IOS Asynchronous Transfer Mode Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Asynchronous Transfer Mode (ATM), including WAN ATM, LAN ATM, and multiprotocol over ATM (MPOA). The command reference provides detailed information about the commands used in the configuration guide.
WAN	
Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 *Cisco IOS Wide-Area Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring wide-area network (WAN) features, including Layer 2 Tunneling Protocol Version 3 (L2TPv3); Frame Relay; Link Access Procedure, Balanced (LAPB); and X.25. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
System Management	
Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to using Cisco IOS software to configure and maintain Cisco routers and access servers, including information about using the Cisco IOS command-line interface (CLI), loading and maintaining system images, using the Cisco IOS file system, using the Cisco IOS Web browser user interface (UI), and configuring basic file transfer services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.4 *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring and managing interfaces and hardware components, including dial shelves, LAN interfaces, logical interfaces, serial interfaces, and virtual interfaces. The command reference provides detailed information about the commands used in the configuration guide.
IBM Technologies	
Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 *Cisco IOS Bridging Command Reference*, Release 12.4 *Cisco IOS IBM Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring: • Bridging features, including transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and Token Ring Route Switch Module (TRRSM). • IBM network features, including data-link switching plus (DLSw+), serial tunnel (STUN), and block serial tunnel (BSTUN); Logical Link Control, type 2 (LLC2), and Synchronous Data Link Control (SDLC); IBM Network Media Translation, including SDLC Logical Link Control (SDLLC) and Qualified Logical Link Control (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. The two command references provide detailed information about the commands used in the configuration guide.
Additional and Legacy Protocols	
Cisco IOS AppleTalk Configuration Guide, Release 12.4 *Cisco IOS AppleTalk Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the AppleTalk protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS DECnet Configuration Guide, Release 12.4 *Cisco IOS DECnet Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the DECnet protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS ISO CLNS Configuration Guide, Release 12.4 *Cisco IOS ISO CLNS Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring International Organization for Standardization (ISO) Connectionless Network Service (CLNS). The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Novell IPX Configuration Guide, Release 12.4 *Cisco IOS Novell IPX Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the Novell Internetwork Packet Exchange (IPX) protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Terminal Services Configuration Guide, Release 12.4 *Cisco IOS Terminal Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring terminal services, including DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). The command reference provides detailed information about the commands used in the configuration guide.

Table 2 lists the documents and resources that support the Cisco IOS Release 12.4 software configuration guides and command references.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources

Document Title	Description
Cisco IOS Master Commands List, Release 12.4	An alphabetical listing of all the commands documented in the Cisco IOS Release 12.4 command references.
Cisco IOS New, Modified, Replaced, and Removed Commands, Release 12.4	A listing of all the new, modified, replaced and removed commands since Cisco IOS Release 12.3, grouped by Release 12.3T maintenance release and ordered alphabetically within each group.
Cisco IOS New and Modified Commands, Release 12.3	A listing of all the new, modified, and replaced commands since Cisco IOS Release 12.2, grouped by Release 12.2T maintenance release and ordered alphabetically within each group.
Cisco IOS System Messages, Volume 1 of 2 *Cisco IOS System Messages, Volume 2 of 2*	Listings and descriptions of Cisco IOS system messages. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference, Release 12.4	An alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, and usage guidelines.
Release Notes, Release 12.4	A description of general release information, including information about supported platforms, feature sets, platform-specific notes, and Cisco IOS software defects.
Internetworking Terms and Acronyms	Compilation and definitions of the terms and acronyms used in the internetworking industry.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources (continued)

Document Title	Description
RFCs	RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/
MIBs	MIBs are used for network monitoring. 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

Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means 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 an SNMP community string to *public*, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords, and are used in contexts in which the italic document convention is not available, such as ASCII text.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

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 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.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation and technical support at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Using Cisco IOS Software for Release 12.4

This chapter provides tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

For an overview of Cisco IOS software configuration, see the *Cisco IOS Configuration Fundamentals Configuration Guide.*

For information on the conventions used in the Cisco IOS software documentation set, see the "About Cisco IOS Software Documentation for Release 12.4" chapter.

Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to a Cisco device, the device is initially in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode by entering the **enable** command and a password (when required). From privileged EXEC mode you have access to both user EXEC and privileged EXEC commands. Most EXEC commands are used independently to observe status or to perform a specific function. For example, **show** commands are used to display important status information, and **clear** commands allow you to reset counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS 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.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
ROM monitor	From privileged EXEC mode, use the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, see the "Using the Cisco IOS Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.

Command	Purpose
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (**?**) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

Table 2 How to Find Command Options

Command	Comment
`Router>` **`enable`** `Password: <password>` `Router#`	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to `Router#`.
`Router#` **`configure terminal`** `Enter configuration commands, one per line. End with CNTL/Z.` `Router(config)#`	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router(config)#`.

Table 2 How to Find Command Options (continued)

<table>
<tr><th>Command</th><th>Comment</th></tr>
<tr><td><pre>Router(config)# interface serial ?
  <0-6>   Serial interface number
Router(config)# interface serial 4 ?
  /
Router(config)# interface serial 4/ ?
  <0-3>   Serial interface number
Router(config)# interface serial 4/0 ?
<cr>
Router(config)# interface serial 4/0
Router(config-if)#</pre></td><td>Enter interface configuration mode by specifying the serial interface that you want to configure using the interface serial global configuration command.

Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.

When the <cr> symbol is displayed, you can press Enter to complete the command.

You are in interface configuration mode when the prompt changes to <code>Router(config-if)#</code>.</td></tr>
<tr><td><pre>Router(config-if)# ?
Interface configuration commands:
  .
  .
  .
  ip   Interface Internet Protocol config commands
  keepalive   Enable keepalive
  lan-name   LAN Name command
  llc2   LLC2 Interface Subcommands
  load-interval   Specify interval for load calculation for an
                      interface
  locaddr-priority   Assign a priority group
  logging   Configure logging for interface
  loopback   Configure internal loopback on an interface
  mac-address   Manually set interface MAC address
  mls   mls router sub/interface commands
  mpoa   MPOA interface configuration commands
  mtu   Set the interface Maximum Transmission Unit (MTU)
  netbios   Use a defined NETBIOS access list or enable
                      name-caching
  no   Negate a command or set its defaults
  nrzi-encoding   Enable use of NRZI encoding
  ntp   Configure NTP
  .
  .
  .
Router(config-if)#</pre></td><td>Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</td></tr>
</table>

Table 2 How to Find Command Options (continued)

Command	Comment
Router(config-if)# **ip ?** Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time . . . Router(config-if)# **ip**	Enter the command that you want to configure for the interface. This example uses the **ip** command. Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.
Router(config-if)# **ip address ?** A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# **ip address**	Enter the command that you want to configure for the interface. This example uses the **ip address** command. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword. A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.
Router(config-if)# **ip address 172.16.0.1 ?** A.B.C.D IP subnet mask Router(config-if)# **ip address 172.16.0.1**	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

Table 2 How to Find Command Options (continued)

Command	Comment
`Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?` `  secondary           Make this IP address a secondary address` `  <cr>` `Router(config-if)# ip address 172.16.0.1 255.255.255.0`	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask. Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**. A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.
`Router(config-if)# ip address 172.16.0.1 255.255.255.0` `Router(config-if)#`	In this example, Enter is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command or the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

command | {**begin** | **include** | **exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
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
```

For more information on the search and filter functionality, see the "Using the Cisco IOS Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

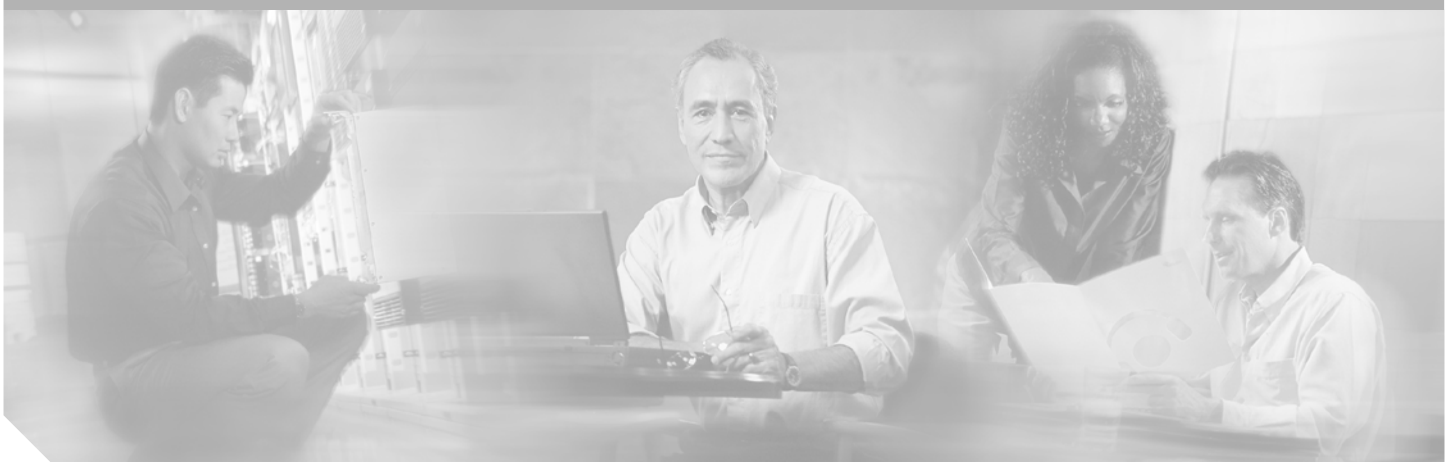
Finding Additional Feature Support Information

If you want to use a specific Cisco IOS software feature, you will need to determine in which Cisco IOS software images that feature is supported. Feature support in Cisco IOS software images depends on three main factors: the software version (called the "Release"), the hardware model (the "Platform" or "Series"), and the "Feature Set" (collection of specific features designed for a certain network environment). Although the Cisco IOS software documentation set documents feature support information for Release 12.4 as a whole, it does not generally provide specific hardware and feature set information.

To determine the correct combination of Release (software version), Platform (hardware version), and Feature Set needed to run a particular feature (or any combination of features), use Feature Navigator.

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.

Software features may also have additional limitations or restrictions. For example, a minimum amount of system memory may be required. Or there may be known issues for features on certain platforms that have not yet been resolved (called "Caveats"). For the latest information about these limitations, see the release notes for the appropriate Cisco IOS software release. Release notes provide detailed installation instructions, new feature descriptions, system requirements, limitations and restrictions, caveats, and troubleshooting information for a particular software release.



Part 1: WAN ATM

Configuring ATM

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
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

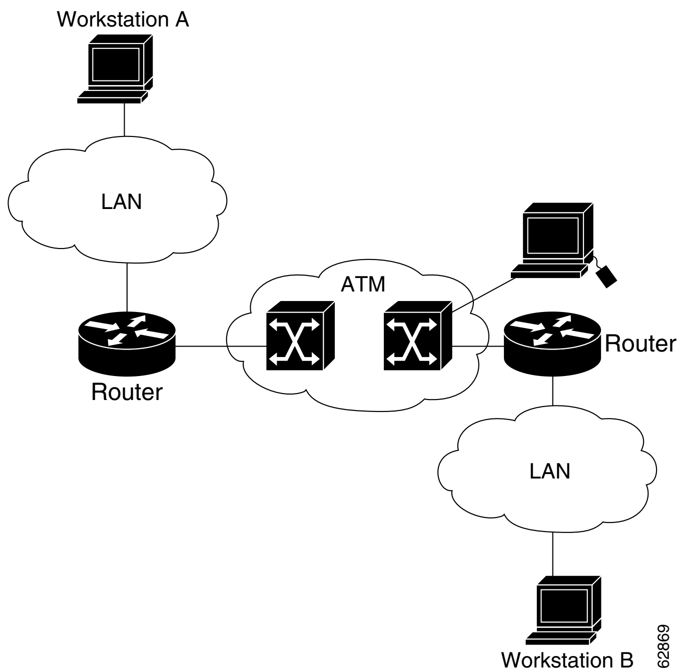
ATM switched virtual circuit (SVC) service operates much like X.25 SVC service, although ATM allows much higher throughput. Virtual circuits are created and released dynamically, providing user bandwidth on demand. This service requires a signalling protocol between the router and the switch.

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.

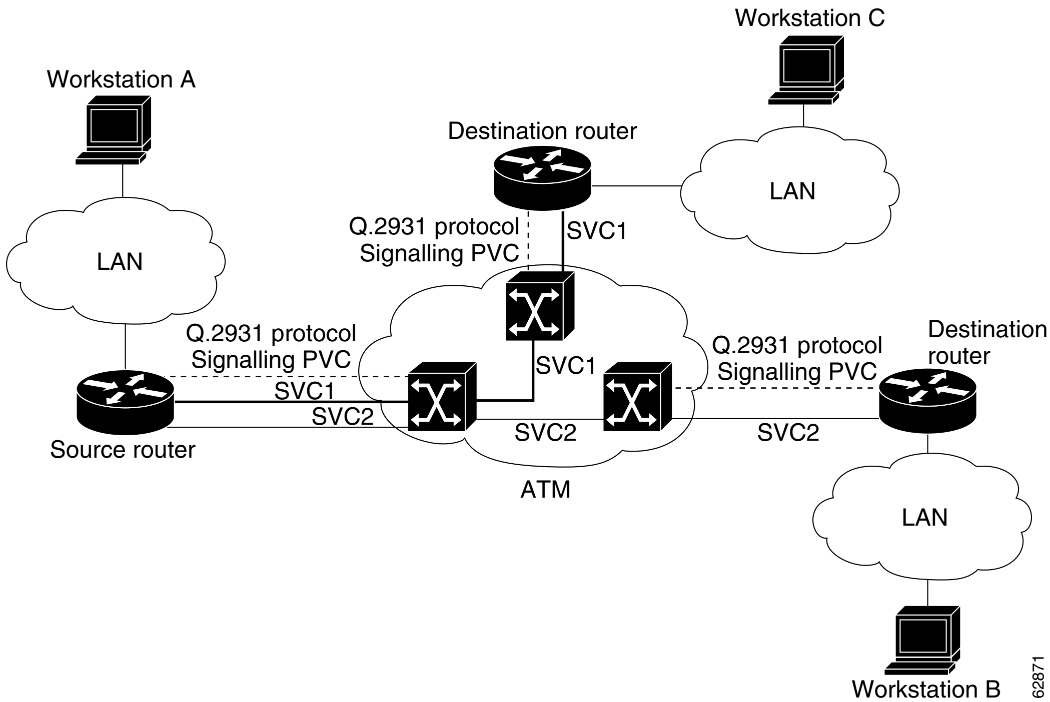
For an example of configuring ILMI, see the section "Configuring Communication with the ILMI Example" in the "ATM Configuration Examples" section at the end of this chapter.

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:

	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
- Limiting the Number of Virtual Circuits
- Setting the Raw-Queue Size
- Configuring Buffer Size
- Setting the VCI-to-VPI Ratio
- Setting the Source of the Transmit Clock

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.
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.
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.

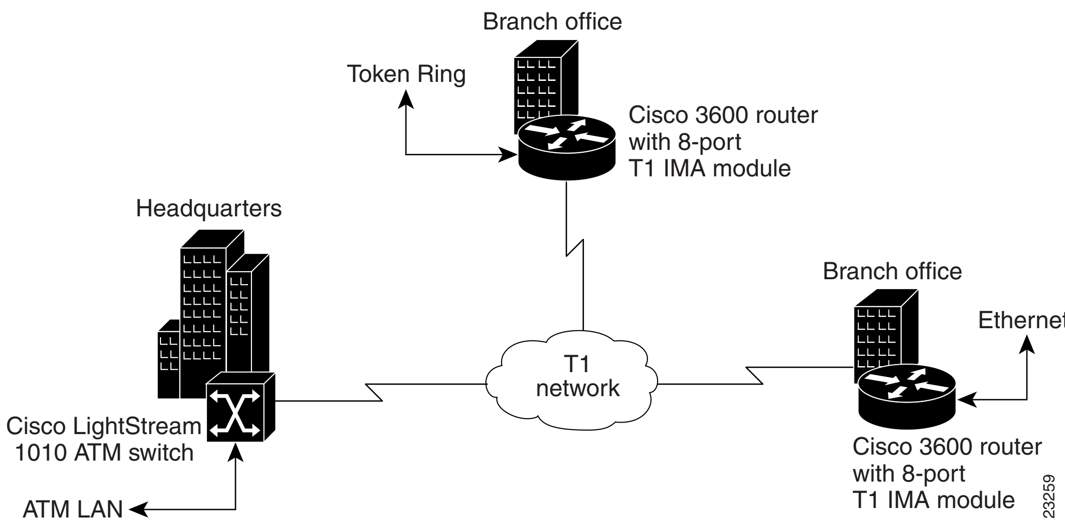
Configuring Inverse Multiplexing over ATM

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

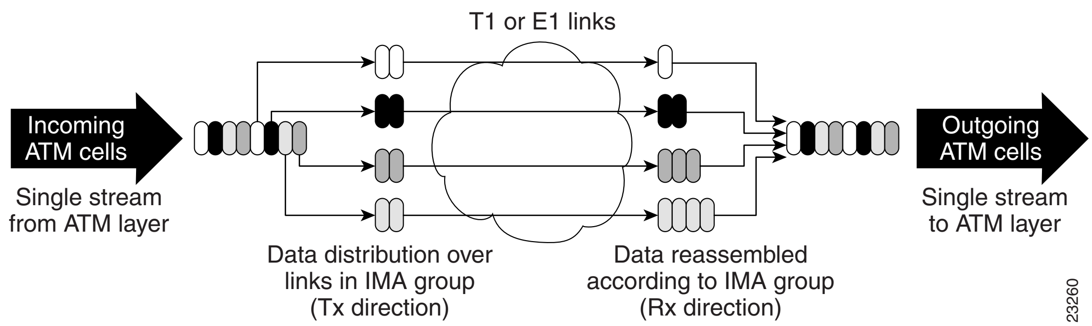
IMA Protocol Overview

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`**`}`	(T1 interfaces only) Sets a cable length longer than 655 feet.
	or	
	`Router(config-if)#` **`cablelength short`** `{`**`133`** `|` **`266`** `|` **`399`** `|` **`533`** `|` **`655`**`}`	(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**} or **lbo short** {**133** | **266** | **399** | **533** | **655**}	Sets a cable length of greater than 655 feet for a T1 link. • **gain26** specifies the decibel pulse gain at 26 decibels. This is the default pulse gain. • **gain36** specifies the decibel pulse gain at 36 decibels. • **-15db** specifies the decibel pulse rate at -15 decibels. • **-22.5db** specifies the decibel pulse rate at -22.5 decibels. • **-7.5db** specifies the decibel pulse rate at -7.5 decibels. • **0db** specifies the decibel pulse rate at 0 decibels. This is the default pulse rate. Sets a cable length of 655 feet or less for a T1 link. There is no default for **lbo short**. • **133** specifies a cable length from 0 to 133 feet. • **266** specifies a cable length from 134 to 266 feet. • **399** specifies a cable length from 267 to 399 feet. • **533** specifies a cable length from 400 to 533 feet. • **655** specifies a cable length from 534 to 655 feet. If you do not set the cable length, the system defaults to a setting of **lbo long gain26 0db (space between gain26 and 0db)**.
Step 4	Router(config-if)# **no ip address**	Disables IP processing. Instead of configuring protocol parameters on the physical interface, you can set these up on the IMA group virtual interface.
Step 5	Router(config-if)# **no atm oversubscribe**	Disables the ATM bandwidth manager, which keeps track of bandwidth used by virtual circuits on a per-interface basis. When you disable bandwidth manager, a check determines whether the ATM link is already oversubscribed. If it is, the command is rejected. Otherwise, the total bandwidth available on the link is recorded and all future connection setup requests are monitored to ensure that the link does not become oversubscribed.

	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.

	Command	Purpose
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.
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 3 and Table 4 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 3 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

Table 3 T1 IMA AAL5 Payload Bandwidth with IMA Frame Size 128 (continued)

Number of Links in the Group	Total Bandwidth	Payload Bandwidth
6	9.216	8.28
7	10.752	9.66
8	12.288	11.04

Table 4 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 5 lists the ATM and E.164 address formats supported by ATM E.164 auto conversion.

Table 5 ATM and E1.64 Address Formats

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

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

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.

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

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:

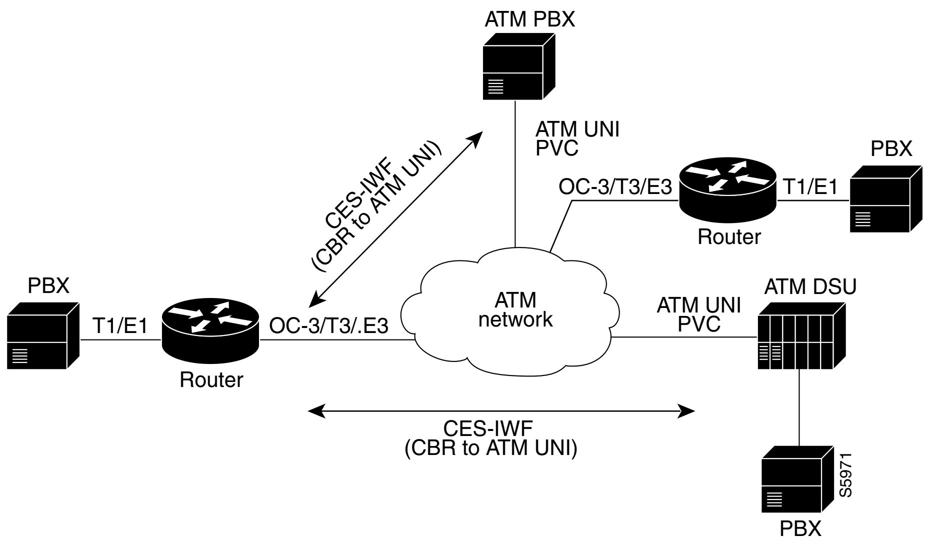
- CES Overview
- Configuring CES on the OC-3/STM-1 ATM Circuit Emulation Service Network Module
- Configuring CES on the ATM-CES Port Adapter
- Configuring Virtual Path Shaping

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.
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.
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.

	Command	Purpose
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.
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.

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

Configuring CES on the ATM-CES Port Adapter

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

- 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_mfCASlt	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.

	Command	Purpose
Step 11	`Router(config-if)#` **`ces pvc`** *`circuit-number`* **`interface atm`** *`slot`***`/`***`port`* **`vpi`** *`number`* **`vci`** *`number`*	Defines the particular ATM destination port for the PVC.
Step 12	`Router(config-if)#` **`no shutdown`**	Changes the shutdown state to up and enables the ATM interface, thereby beginning the segmentation and reassembly (SAR) operation on the interface.
Step 13	`Router(config-if)#` **`no ces circuit`** *`circuit-number`* **`shutdown`**	Enables the PVC.

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 The number of CES PVCs that are multiplexed depends on the bandwidth requirement. Because of this requirement, the CES PVCs cannot be oversubscribed. The CES PVC will fail if there is no bandwidth available. Data PVCs use the bandwidth that is unused by the CES PVCs.

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.
Step 4	`Router(config)# interface cbr slot/port` `ces circuit circuit-number` `ces pvc circuit-number interface atm slot/port vpi number vci number`	(Optional) Creates a CES PVC with a VPI that matches the VPI specified in Step 1.

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`*`]`	Displays all active ATM virtual circuits (PVCs and SVCs) and traffic information.
`Router#` **`show controllers atm`** `[`*`slot`***`/ima`** *`group-number`*`]`	Displays information about current settings and performance at the physical level.

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

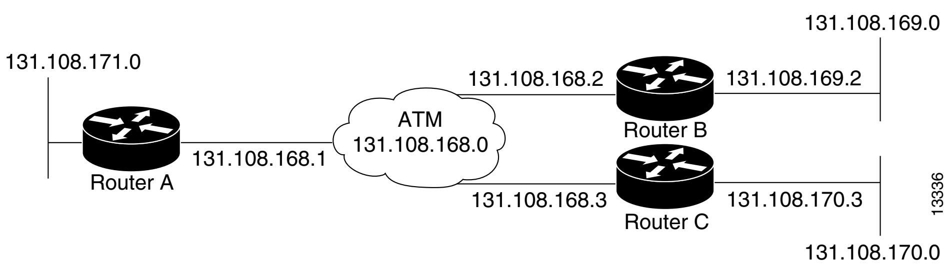
```
interface atm 4/0
 ip address 172.21.168.112 255.255.255.0
 atm maxvc 512
 pvc 1/51
 protocol ip 171.21.168.110
 exit
!
 pvc 2/52
 protocol decnet 10.1 broadcast
 exit
!
 pvc 3/53
 protocol clns 47.004.001.0000.0c00.6e26.00 broadcast
 exit
!
 decnet cost 1
 clns router iso-igrp comet
 exit
!
router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

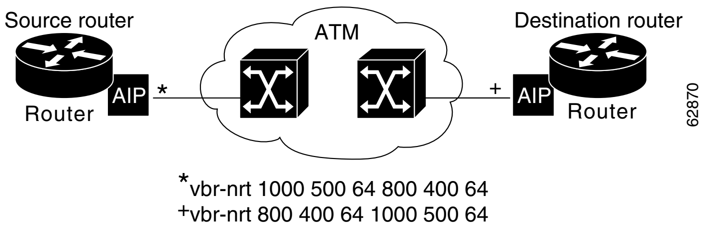
```
interface atm 2/0
 ip address 4.4.4.6 255.255.255.0
 pvc 0/5 qsaal
 exit
!
 pvc 0/16 ilmi
 exit
!
 atm esi-address 3456.7890.1234.12
!
 svc mcast-1 nsap cd.cdef.01.234566.890a.bcde.f012.3456.7890.1234.12 broadcast
 protocol ip 4.4.4.4 broadcast
 exit
!
 svc mcast-2 nsap 31.3233.34.352637.3839.3031.3233.3435.3637.3839.30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

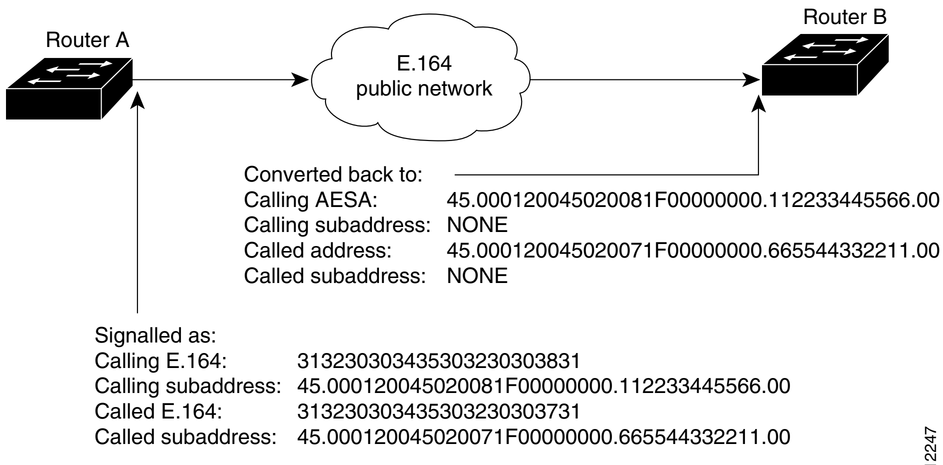
Configuring ATM E.164 Auto Conversion Example

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
```

ATM OAM Ping

The ATM OAM Ping feature sends an ATM Operation, Administration, and Maintenance (OAM) packet to confirm the connectivity of a specific permanent virtual circuit (PVC). The status of the PVC is displayed when a response to the OAM packet is received. The ATM OAM Ping feature allows the network administrator to verify PVC integrity and facilitates ATM network troubleshooting.

Feature History for the ATM OAM Ping Feature

Release	Modification
12.0(21)S	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Prerequisites for ATM OAM Ping

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 Wide-Area Networking Configuration Guide*, Release 12.3.

Restrictions for ATM OAM Ping

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 ATM OAM Ping

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

- Uses for ATM OAM Ping Command, page 106

Uses for ATM OAM Ping Command

The ATM OAM Ping feature modifies the **ping** command, which can be used to send an OAM packet to verify the 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 the 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 ATM OAM Ping

See the following sections for tasks that use **ping** commands to test network connectivity in an ATM network. The tasks in this list are optional.

- Testing Network Connectivity Using ATM Interface Ping (Normal Mode)
- Testing Network Connectivity Using ATM Interface Ping (Interactive Mode)
- Aborting a Ping Session

Testing Network Connectivity Using ATM Interface Ping (Normal Mode)

The task in this section tests network connectivity 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** [*repeat* [*timeout*]] | **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** [*repeat* [*timeout*]] | **seg-loopback** [*repeat* [*timeout*]]] **Example:** `Router# ping atm interface atm1/1.1 0 500 end-loopback 1 2`	Displays a response to confirm the connectivity of a specific PVC. • **atm** *interface-number*—ATM interface name. • *vpi-value*—Virtual path identifier. Range: 0 to 255. • *vci-value*—Virtual channel identifier. Range: 0 to 65535. • **end-loopback**—Sends ATM end loopback cells. This is the default. • **seg-loopback**—Sends ATM segment loopback cells. • *repeat*—Number of ping packets that are sent to the destination. Range: 1 to 1000. Default: 5. • *timeout*—Timeout interval, in seconds. Range: 1 to 30. Default: 2.

Testing Network Connectivity Using ATM Interface Ping (Interactive Mode)

The task in this section tests network connectivity using the **ping** command by providing inputs in the interactive mode; that is, by providing values for the **ping** test by typing the value after the prompts displayed and pressing the Enter key. Press the Enter key without supplying a value to use the default.

SUMMARY STEPS

1. **enable**
2. **ping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
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—by default, **Ctrl-Shift-6**.

Configuration Examples for ATM OAM Ping

This section provides the following configuration examples:

- Verifying the Connectivity of a Specific PVC: Example, page 108
- Normal Mode ping atm interface atm Command: Example, page 109
- Interactive ping Command: Example, page 110

Verifying the Connectivity of a Specific PVC: Example

The following example helps verify 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
```

Normal Mode ping atm interface atm Command: Example

The following example shows 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
```

Interactive ping Command: 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	"Creating PVCs" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.3
Configuring ATM	"Configuring ATM" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.3
WAN commands, complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Wide-Area Networking Command Reference*, Release 12.3
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

Standards

Standards	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

MIBs	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

Modified Command

- **ping atm interface atm**

ATM OAM Support for F5 Continuity Check

Feature History

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

This document describes the ATM OAM Support for F5 Continuity Check feature in Cisco IOS Release 12.2(13)T. It includes the following sections:

Feature Overview

The ATM OAM Support for F5 Continuity Check feature introduces Operation, Administration, and Maintenance (OAM) support for the use of F5 segment and end-to-end continuity check (CC) cells to detect connectivity failures at the ATM layer. This feature also introduces new Simple Network Management Protocol (SNMP) notifications that are generated when CC cells indicate virtual circuit (VC) connectivity failure.

ATM OAM F5 CC cells provide an in-service tool optimized to detect connectivity problems at the VC level of the ATM layer. CC cells are sent between a router designated as the source location and a router designated as the sink location. The local router can be configured as the source, as the sink, or as both the source and the sink.

This feature implements two types of OAM cells: CC cells for fault management and CC cells for activation and deactivation. Fault management cells detect connectivity failures. Activation and deactivation cells initiate the activation or deactivation of continuity checking.

SNMP Support for ATM OAM F5 Continuity Checking

The ATM OAM Support for F5 Continuity Check feature introduces three new SNMP notifications that indicate CC segment, CC end-to-end, and alarm indication signal/remote defect indication (AIS/RDI) failures to the network management system (NMS). The notifications include information such as the number of OAM failures that occurred and time stamps showing when the first and last failures occurred during the notification interval for permanent virtual circuits (PVCs). In addition to notifications, MIB tables are maintained to provide information about the failures on PVCs.

For a complete description of the extended ATM PVC 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/public/sw-center/netmgmt/cmtk/mibs.shtml

Benefits

The ATM OAM Support for F5 Continuity Check feature enables network administrators to detect connectivity failures on a per-PVC basis. The feature also provides support for SNMP notifications that notify the administrator that continuity for a particular PVC has been lost while the PVC is still operationally up.

Restrictions

Cisco digital subscriber line access multiplexers (DSLAMs) and ATM switches (such as the Cisco LS1010) do not forward F5 OAM segment CC cells.

The ATM OAM Support for F5 Continuity Check feature is supported on ATM PVCs only.

Related Documents

For more information on configuring OAM and ATM PVC trap support, refer to the following documents:

- The “Configuring ATM” chapter of the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2
- The “ATM Commands” chapter of the *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2

For information on configuring SNMP, refer to the following documents:

- The “Configuring SNMP Support” chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- The “SNMP Commands” chapter of the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2

Supported Platforms

- Cisco 827
- Cisco 1700 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

The MIB that supports ATM OAM F5 CC management is defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my.

The MIB that supports legacy extended ATM PVC traps is defined in the file CISCO-IETF-ATM2-PVCTRAP-MIB.my.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Extended ATM PVC and ATM OAM F5 CC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps and ATM OAM F5 CC traps can be configured. If the extended ATM PVC traps or ATM OAM F5 CC traps are enabled, you must disable them by using the **no snmp-server enable traps atm pvc extension** command before you can enable the legacy ATM PVC trap.

Configuration Tasks

See the following sections for configuration tasks for the ATM OAM Support for F5 Continuity Check feature. Each task in the list is identified as either required or optional.

- Configuring ATM OAM F5 CC Support (required)
- Configuring Denial of ATM OAM F5 CC Activation Requests (optional)
- Configuring ATM OAM F5 CC Deactivation Requests to Be Sent upon PVC Failure (optional)
- Configuring SNMP Notification Support for ATM OAM F5 CC Management (required)
- Verifying ATM OAM Support for F5 CC Management (optional)

Configuring ATM OAM F5 CC Support

To configure ATM OAM F5 CC support on an ATM PVC, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`interface atm`** *`number`*	Specifies an interface for configuration and enters interface configuration mode.
Step 2	`Router(config-if)#` **`ip address`** *`ip-address mask`*	Sets a primary or secondary IP address for an interface.

	Command	Purpose
Step 3	Router(config-if)# **pvc** [*name*] *vpi*/*vci*	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 4	Router(config-if-atm-vc)# **oam-pvc manage cc** {**end** | **segment**} [**direction** {**both** | **sink** | **source**}] [**keep-vc-up** [**end aisrdi failure** | **seg aisrdi failure**]]	Configures ATM OAM F5 CC management.
Step 5	Router(config-if-atm-vc)# **oam retry cc** {**end** | **segment**} [*activation-count* [*deactivation-count* [*retry-frequency*]]]	Sets the retry count and the frequency at which CC activation and deactivation requests are sent to the device at the other end of the PVC or the segment.

Configuring Denial of ATM OAM F5 CC Activation Requests

To disable ATM OAM F5 CC support on an ATM PVC and to configure the PVC to deny OAM F5 CC activation requests, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **interface atm** *number*	Specifies an interface for configuration and enters interface configuration mode.
Step 2	Router(config-if)# **ip address** *ip-address mask*	Sets a primary or secondary IP address for an interface.
Step 3	Router(config-if)# **pvc** [*name*] *vpi*/*vci*	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 4	Router(config-if-atm-vc)# **oam-pvc manage cc** {**end** | **segment**} **deny**	Disables ATM OAM F5 CC support by configuring the VC to deny CC activation requests.

Configuring ATM OAM F5 CC Deactivation Requests to Be Sent upon PVC Failure

To configure a PVC to send ATM OAM F5 CC deactivation requests when the PVC is already down, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **interface atm** *number*	Specifies an interface for configuration and enters interface configuration mode.
Step 2	Router(config-if)# **ip address** *ip-address mask*	Sets a primary or secondary IP address for an interface.
Step 3	Router(config-if)# **pvc** [*name*] *vpi*/*vci*	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 4	Router(config-if-atm-vc)# **no oam-pvc manage cc** {**end** | **segment**} [**deactivate-down-vc**]	Configures the PVC to send deactivation requests if the PVC is already in down state.

Configuring SNMP Notification Support for ATM OAM F5 CC Management

To enable the MIB and the sending of SNMP notifications that support ATM OAM F5 CC management, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **snmp-server enable traps atm pvc extension mibversion 2**	Specifies the MIB that supports the SNMP notifications for ATM OAM F5 CC management.
Step 2	Router(config)# **snmp-server enable traps atm pvc extension** {**up** | **down** | **oam failure** [**aisrdi** | **endCC** | **loopback** | **segmentCC**]}	Enables the sending of extended ATM PVC, ATM OAM F5 CC, ATM OAM F5 AIS/RDI, and ATM OAM F5 Loopback SNMP notifications.

Verifying ATM OAM Support for F5 CC Management

To verify the configuration and operation of ATM OAM F5 CC management, perform the following steps:

Step 1 Use the **show running-config** command to verify configuration. The following is sample output for the **show running-config** command:

```
Router# show running-config interface atm0

Building configuration...

Current configuration :152 bytes
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 pvc 1/40
  oam-pvc manage cc segment direction both
 !
 dsl operating-mode auto
end
```

Step 2 Use the **show atm pvc** command to verify that ATM OAM F5 CC management is enabled and to display the activation and deactivation retry counts and retry frequency values. This command also displays the CC state of the PVC.

The following is sample output for the **show atm pvc** command:

```
Router# show atm pvc 1/40

ATM0:VCD:1, VPI:1, VCI:40
UBR, PeakRate:0
AAL5-LLC/SNAP, etype:0x0, Flags:0xC20, VCmode:0x0
OAM frequency:0 second(s), OAM retry frequency:1 second(s)
OAM up retry count:3, OAM down retry count:5
OAM END CC Activate retry count:3, OAM END CC Deactivate retry count:3
OAM END CC retry frequency:30 second(s),
OAM SEGMENT CC Activate retry count:3, OAM SEGMENT CC Deactivate retry count:3
OAM SEGMENT CC retry frequency:30 second(s),
OAM Loopback status:OAM Disabled
OAM VC state:Not Managed
ILMI VC state:Not Managed
```

```
OAM END CC status:OAM CC Ready
OAM END CC VC state:Verified
OAM SEGMENT CC status:OAM CC Active
OAM SEGMENT CC VC state:Verified
InARP frequency:15 minutes(s)
InPkts:0, OutPkts:0, InBytes:0, OutBytes:0
InPRoc:0, OutPRoc:0, Broadcasts:0
InFast:0, OutFast:0, InAS:0, OutAS:0
Giants:0
OAM cells received:20
F5 InEndloop:0, F5 InSegloop:0,
F5 InEndcc:0, F5 InSegcc:20, F5 InAIS:0, F5 InRDI:0
F4 InEndloop:0, F4 InSegloop:0, F4 InAIS:0, F4 InRDI:0
OAM cells sent:20
F5 OutEndloop:0, F5 OutSegloop:0,
F5 OutEndcc:0, F5 OutSegcc:20, F5 OutRDI:0
F4 OutEndloop:0, F4 OutSegloop:0, F4 OutRDI:0
OAM cell drops:1
Status:UP
```

Monitoring and Maintaining ATM OAM F5 CC Management

To monitor and maintain ATM OAM F5 continuity checking, use the following command in privileged EXEC mode:

Command	Purpose
Router# **debug atm oam cc**	Displays ATM OAM F5 continuity checking activity.

Configuration Examples

This section provides the following configuration examples:

- ATM OAM F5 CC Support on a PVC Configuration Example
- Denial of ATM OAM F5 CC Activation Requests Configuration Example
- Deactivation of ATM OAM F5 CC upon PVC Failure Example
- Support for ATM OAM F5 CC SNMP Notifications Configuration Example

ATM OAM F5 CC Support on a PVC Configuration Example

The following example shows how to configure ATM OAM CC support over the segment and configure the router to function as the source. The frequency at which CC activation and deactivation requests will be sent over the segment is also configured.

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  oam-pvc manage cc segment direction source
  oam retry cc segment 10 10 30
```

Denial of ATM OAM F5 CC Activation Requests Configuration Example

The following example shows how to disable ATM OAM F5 CC support and configure the VC to deny CC activation requests:

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  oam-pvc manage cc segment deny
```

Deactivation of ATM OAM F5 CC upon PVC Failure Example

The following example shows how to send a CC deactivation request across the segment when PVC 0/40 goes down:

```
interface atm 0
 ip address 10.0.0.3 255.255.255.0
 pvc 0/40
  no oam-pvc manage cc segment deactivate-down-vc
```

Support for ATM OAM F5 CC SNMP Notifications Configuration Example

In the following example, the ATM OAM F5 CC notifications and an extended ATM PVC notification are enabled. If CC cells detect connectivity failures on PVC 0/40, host 172.16.61.90 will receive the SNMP notifications.

```
! Configure SNMP support on your router:
snmp-server community public
snmp-server host 172.16.61.90 public
!
! Enable SNMP notifications:
snmp-server enable traps atm pvc extension mibversion 2
snmp-server enable traps atm pvc extension oam failure aisrdi
snmp-server enable traps atm pvc extension oam failure endcc
snmp-server enable traps atm pvc extension oam failure segmentcc
snmp-server enable traps atm pvc extension oam failure loopback
snmp-server enable traps atm pvc extension up
```

Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **debug atm oam cc**
- **oam-pvc manage cc**
- **oam-pvc manage cc deny**
- **oam retry cc**
- **snmp-server enable traps atm pvc extension**
- **snmp-server enable traps atm pvc extension mibversion**

Glossary

AIS—alarm indication signal. In a T1 transmission, an all-ones signal transmitted in lieu of the normal signal to maintain transmission continuity and to indicate to the receiving terminal that there is a transmission fault that is located either at or upstream from the transmitting terminal.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system (NMS).

NMS—network management system. An application or suite of applications designed to monitor networks using SNMP.

OAM—Operation, Administration, and Maintenance. OAM cells provide a virtual-circuit-level loopback in which a router responds to the cells, demonstrating that the circuit is up and the router is operational.

PVC—permanent virtual circuit. Virtual circuit that is permanently established. In ATM terminology, PVC also stands for permanent virtual connection.

RDI—remote defect indication. In ATM, when the physical layer detects loss of signal or cell synchronization, RDI cells are used to report a virtual path connection/virtual channel connection (VPC/VCC) failure. RDI cells are sent upstream by a VPC/VCC endpoint to notify the source VPC/VCC endpoint of the downstream failure.

SNMP—Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents and is used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

SNMP trap—Message from an SNMP agent alerting the SNMP manager to a condition on the network.

ATM Policing by Service Category for SVC/SoftPVC

Feature History

Release	Modification
12.2(4)B	This feature was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

This document describes the ATM Policing by Service Category for SVC/SoftPVC feature in Cisco IOS Release 12.2(13)T and includes the following sections:

Feature Overview

When configured, an ATM switch at the network side of a user-to-network (UNI) interface polices the flow of cells in the forward (into the network) direction of a virtual connection. These traffic policing mechanisms are known as usage parameter control (UPC). With UPC, the switch determines whether received cells comply with the negotiated traffic management values and takes one of the following actions on violating cells:

- Pass the cell without changing the cell loss priority (CLP) bit in the cell header.
- Tag the cell with a CLP bit value of 1.
- Drop (discard) the cell.

The ATM Policing by Service Category for SVC/SoftPVC feature enables you to specify which traffic to police, based on service category, on switched virtual circuits (SVCs) or terminating VCs on the destination end of a soft VC.

For more information on UPC, see the "Traffic and Resource Management" chapter in the *Guide to ATM Technology*.

Benefits

This feature enables you to select which and how traffic is affected by UPC. For example, you can configure your switch to pass all UBR traffic, but tag all other traffic types.

Related Features and Technologies

- Intelligent early packet discard (EPD)
- Intelligent partial (tail) packet discard

Related Documents

- *ATM Switch Router Software Configuration Guide*
- *ATM and Layer 3 Switch Router Command Reference*
- *Guide to ATM Technology*
- *ATM Forum UNI 3.1 Specification*

Supported Platforms

This feature is supported on the node switch processor (NSP) of the Cisco 6400 carrier-class broadband aggregator.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

CISCO-ATM-IF-MIB.my—New objects were created for per-service category SVC UPC intent.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

None

Configuration Tasks

See the following sections for configuration tasks for the ATM Policing by Service Category for SVC/SoftPVC feature. Each task in the list is identified as either required or optional:

- Configuring ATM Policing by Service Category for SVC/SoftPVC (Required)
- Verifying ATM Policing by Service Category for SVC/SoftPVC (Optional)

Configuring ATM Policing by Service Category for SVC/SoftPVC

To configure the ATM Policing by Service Category for SVC/SoftPVC feature, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)#` **`interface atm`** *`slot/subslot/port`*	Selects the ATM interface.
Step 2	`Switch(config-if)#` **`atm svc-upc-intent`** `[{`**`abr`** `|` **`cbr`** `|` **`vbr-rt`** `|` **`vbr-nrt`** `|` **`ubr`**`}]` `{`**`tag`** `|` **`pass`** `|` **`drop`**`}` (Repeat this step for each service category and UPC mode combination.)	Specifies the UPC mode. If no service category is specified, then the UPC mode configuration is applied to all traffic types.

Verifying ATM Policing by Service Category for SVC/SoftPVC

Step 1 Enter the **show atm vc** or **show atm vp** EXEC command to display the UPC mode for a particular VC or VP.

```
Switch# show atm vc int atm 0/0/1 2 120

Interface:ATM0/0/1, Type:oc3suni
VPI = 2  VCI = 120
Status:DOWN
Time-since-last-status-change:1w1d
Connection-type:PVC
Cast-type:point-to-multipoint-leaf
Packet-discard-option:disabled
Usage-Parameter-Control (UPC):pass
Wrr weight:2
Number of OAM-configured connections:0
OAM-configuration:disabled
OAM-states: Not-applicable
Cross-connect-interface:ATM0/0/1, Type:oc3suni
...
```

Step 2 Enter the **show atm interface** EXEC command. If the UPC mode is not the same for all service categories, the "Svc Upc Intent" field displays "by sc."

```
Switch# show atm interface atm 8/0/1

Interface:     ATM8/0/1        Port-type:     oc3suni
IF Status:     UP              Admin Status:  up
Auto-config:   enabled         AutoCfgState:  completed
IF-Side:       Network         IF-type:       NNI
Uni-type:      not applicable  Uni-version:   not applicable
Max-VPI-bits:  8               Max-VCI-bits:  14
Max-VP:        255             Max-VC:        16383
ConfMaxSvpcVpi:255             CurrMaxSvpcVpi:255
ConfMaxSvccVpi:255             CurrMaxSvccVpi:255
ConfMinSvccVci:35              CurrMinSvccVci:35
Svc Upc Intent:by sc           Signalling:    Enabled
ATM Address for Soft VC:47.0091.8100.0000.0002.b9ae.9301.4000.0c84.0010.00
Configured virtual links:
  PVCLs SoftVCLs   SVCLs   TVCLs   PVPLs SoftVPLs   SVPLs Total-Cfgd Inst-Conns
      3        4       0       0       1        0       0          8          7
Logical ports(VP-tunnels):    0
Input cells:   3036674         Output cells:  3036816
5 minute input rate:            0 bits/sec,       0 cells/sec
5 minute output rate:           0 bits/sec,       0 cells/sec
Input AAL5 pkts:1982638, Output AAL5 pkts:1982687, AAL5 crc errors:0
```

Troubleshooting Tips

If a VC is not configured with the appropriate UPC mode, make sure that the VC was set up after the **atm svc-upc-intent** command was configured. Changes to the UPC mode take affect after the VC is torn down and set up again.

Monitoring and Maintaining ATM Policing by Service Category for SVC/SoftPVC

Use the commands listed below to monitor and maintain ATM Policing by Service Category for SVC/SoftPVC:

Command	Purpose
Switch# **show atm interface**	Displays ATM-specific information about an ATM interface.
Switch# **show controllers atm** *slot***/***subslot***/***port*	Displays information about a physical port device. Includes dropped (or discarded) cells.
Switch# **show atm vc** [**interface atm** *slot***/***subslot***/***port*]	Displays the configured UPC action and intelligent packet discard mechanisms, as well as the number of cells discarded due to UPC violations.

Example: Monitoring and Maintaining ATM Policing by Service Category for SVC/SoftPVC

```
Switch# show atm vc interface atm 3/0/1.51 51 16

     Interface: ATM3/0/1.51, Type: oc3suni
     VPI = 51  VCI = 16
     Status: DOWN
     Time-since-last-status-change: 2w0d
     Connection-type: PVC
     Cast-type: point-to-point
     Packet-discard-option: enabled
     Usage-Parameter-Control (UPC): pass
     Wrr weight: 32
     Number of OAM-configured connections: 0
     OAM-configuration: disabled
     OAM-states:  Not-applicable
     Cross-connect-interface: ATM2/0/0, Type: ATM Swi/Proc
     Cross-connect-VPI = 0
     Cross-connect-VCI = 73
     Cross-connect-UPC: pass
     Cross-connect OAM-configuration: disabled
     Cross-connect OAM-state:  Not-applicable
     Encapsulation: AAL5ILMI
     Threshold Group: 6, Cells queued: 0
     Rx cells: 0, Tx cells: 0
     Tx Clp0:0,  Tx Clp1: 0
     Rx Clp0:0,  Rx Clp1: 0
     Rx Upc Violations:0, Rx cell drops:0
     Rx pkts:0, Rx pkt drops:0
     Rx connection-traffic-table-index: 6
     Rx service-category: UBR (Unspecified Bit Rate)
     Rx pcr-clp01: 424
     Rx scr-clp01: none
     Rx mcr-clp01: none
     Rx      cdvt: 1024 (from default for interface)
     Rx       mbs: none
     Tx connection-traffic-table-index: 6
     Tx service-category: UBR (Unspecified Bit Rate)
     Tx pcr-clp01: 424
     Tx scr-clp01: none
     Tx mcr-clp01: none
     Tx      cdvt: none
     Tx       mbs: none
     No AAL5 connection registered
```

Configuration Examples

This section provides the following configuration example:

- Non-UBR Traffic Policing

Non-UBR Traffic Policing

In the following example, the UBR traffic on ATM 3/0/0 is passed while all other traffic is policed:

```
Switch(config)# interface atm 3/0/0
Switch(config-if)# atm svc-upc-intent ubr pass
Switch(config-if)# atm svc-upc-intent cbr tag
Switch(config-if)# atm svc-upc-intent vbr-rt tag
Switch(config-if)# atm svc-upc-intent vbr-nrt tag
Switch(config-if)# atm svc-upc-intent abr drop
```

Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **atm svc-upc-intent**

Glossary

ABR—available bit rate. QoS class defined by the ATM Forum for ATM networks. ABR is used for connections that do not require timing relationships between source and destination. ABR provides no guarantees in terms of cell loss or delay, providing only best-effort service. Traffic sources adjust their transmission rate in response to information they receive describing the status of the network and its capability to successfully deliver data. Compare with CBR, UBR, and VBR.

CBR—constant bit rate. QoS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery. Compare with ABR, UBR, and VBR.

CLP—cell loss priority. Field in the ATM cell header that determines the probability of a cell being dropped if the network becomes congested. Cells with CLP = 0 are insured traffic, which is unlikely to be dropped. Cells with CLP = 1 are best-effort traffic, which might be dropped in congested conditions to free up resources to handle insured traffic.

PVC—permanent virtual circuit (or connection). Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection. Compare with SVC. See also virtual circuit.

soft PVC—A PVC-SVC hybrid in which only the two terminating virtual connection links (VCLs) at either end are permanent and the rest of the VCLs are switched (SVC). Like the PVC, a soft PVC is permanent and the called party cannot drop the connection. Like the SVC, a soft PVC is automatically rerouted if a switch or link in the path fails.

SVC—switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. See also virtual circuit. Called a switched virtual connection in ATM terminology. Compare with PVC.

tagged traffic—ATM cells that have their CLP bit set to 1. If the network is congested, tagged traffic can be dropped to ensure the delivery of higher-priority traffic. Sometimes called DE traffic. See also CLP.

traffic policing—Process used to measure the actual traffic flow across a given connection and compare it to the total admissible traffic flow for that connection. Traffic outside of the agreed upon flow can be tagged (where the CLP bit is set to 1) and can be discarded en route if congestion develops. Traffic policing is used in ATM, Frame Relay, and other types of networks. Also known as admission control, permit processing, rate enforcement, and UPC. See also tagged traffic.

UBR—unspecified bit rate. QoS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network but there are no guarantees in terms of cell loss rate and delay. Compare with ABR, CBR, and VBR.

UPC—usage parameter control. See traffic policing.

VBR—variable bit rate. QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

virtual circuit—Logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC). Virtual circuits are used in Frame Relay and X.25. In ATM, a virtual circuit is called a virtual channel. Sometimes abbreviated VC.

ATM SNMP Trap and OAM Enhancements

Feature History

Release	Modification
12.2(4)T	This feature was introduced.
12.2(4)T3	Support for Cisco 7500 series routers was added.

This document describes the ATM SNMP Trap and OAM Enhancements feature in Cisco IOS Release 12.2(4)T. It includes the following sections:

Feature Overview

The ATM SNMP Trap and OAM Enhancements feature introduces the following enhancements to the Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) and to Operation, Administration, and Maintenance (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. Additionally, when OAM loopback fails, the PVC will now remain in the UP state, rather than going down.
- The ATM PVC traps are now extended to include virtual path identifier/virtual channel indentifier (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.

The ATM SNMP trap and OAM enhancements are described in the following sections:

- ATM PVC Up Trap
- ATM PVC OAM Failure Trap
- Extended ATM PVC Traps
- Supported MIB Objects and Tables

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, which 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 introduce 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 the introduction of this feature, if OAM loopback failed, the PVC would be placed in the down state. When the ATM PVC OAM failure trap is enabled, the PVC remains up when OAM loopback fails so that the flow of data will still be possible.

Note ATM PVC traps are generated at the end of the notification interval. It is possible to generate all 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 will be 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 extended ATM PVC traps can be configured.

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 have gone 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

For a complete description of the extended ATM PVC MIB, see the MIB file called CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my, available through Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Benefits

The ATM SNMP Trap and OAM enhancements

- Enable you to use SNMP to detect the recovery of PVCs that have gone down.
- Enable you to use SNMP to detect when OAM loopback for a PVC has failed.
- Keep the PVC in the up state when OAM loopback has failed, allowing for the continued flow of data.

- Provide VPI/VCI information in the ATM PVC traps, letting you know which PVC has changed operational state or has had an OAM loopback failure.
- Provide statistics on the number of state transitions a PVC goes through.

Restrictions

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 extended ATM PVC traps can be configured.

ATM PVC UP traps are not generated for newly created PVCs. They are generated only for PVCs that go from the down state to the up state.

Related Documents

For more information on configuring OAM and ATM PVC trap support, see the following documents:

- The "Configuring ATM" chapter of the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2.
- The "ATM Commands" chapter of the *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2.

For information on configuring SNMP, see the following documents:

- The "Configuring SNMP Support" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- The "SNMP Commands" chapter of the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2

Supported Platforms

- Cisco 2600 series
- Cisco 3660
- Cisco 7200 series
- Cisco 7500 series (Cisco IOS Release 12.2(4)T3 and later)

Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

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

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

This feature provides enhancements to the ATM PVC trap MIB. The MIB file CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my can be downloaded from the Cisco MIB website on Cisco.com at

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Before you enable 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 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 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 extended ATM PVC traps can be configured.

Configuration Tasks

See the following sections for configuration tasks for the ATM SNMP trap and OAM enhancements. Each task in the list is identified as either optional or required.

- Configuring Extended ATM PVC Trap Support (required)
- Enabling OAM Management (required)

- Verifying ATM PVC Traps (optional)

Configuring Extended ATM PVC Trap Support

To configure extended ATM PVC trap support, use the following command in global configuration mode:

Command	Purpose
Router(config)# **snmp-server enable traps atm pvc extension** {**up** | **down** | **oam failure loopback**}	Enables the sending of extended ATM PVC traps. The keywords are as follows: • **up**—Enables ATM PVC up traps, which are generated when a PVC changes from the down to up state. • **down**—Enables ATM PVC failure traps, which are generated when a PVC changes from the up to down state. • **oam failure loopback**—Enables ATM PVC OAM failure traps, which are generated when OAM loopback fails.

Enabling OAM Management

When you configure PVC trap support, you must also enable OAM management on the PVC. To enable OAM management, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 3	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 4	Router(config-if)# **pvc** [*name*] *vpi*/*vci*	Enables the PVC.
Step 5	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.

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.

Monitoring and Maintaining ATM PVC Traps

To monitor ATM PVC trap performance, use the following commands in EXEC mode:

Command	Purpose
`Router# debug atm errors`	Displays ATM errors.
`Router# debug atm oam`	Displays information about ATM OAM events.
`Router# debug snmp packets`	Displays information about every SNMP packet sent or received by the router.

Configuration Examples

This section provides the following configuration example:

- Configuring Extended ATM PVC Trap Support: Example
- Extended ATM PVC Traps Output: Examples

Configuring Extended ATM PVC Trap Support: Example

The following example shows all three of the extended ATM PVC traps enabled on a router. If PVC 0/1 leaves the up state, leaves the down state, or has an OAM loopback failure, host 172.16.61.90 will receive the 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: Example

The following example shows 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, which generates a separate trap for each PVC). The VPI/VCI information and timing information 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
atmPVclStatusChangeEnd.19.1.100 = 140636
00:23:56:SNMP:Packet sent via UDP to 1.1.1.1
```

Extended ATM PVC Up Trap Output: Example

The following example shows 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
00:31:30:SNMP:Packet sent via UDP to 1.1.1.1
```

Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **snmp-server enable traps atm pvc extension**

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 used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

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.

ATM SVC Troubleshooting Enhancements

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the ATM SVC Troubleshooting Enhancements feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

Feature Overview

The ATM SVC Troubleshooting Enhancements feature introduces two new debug commands: **debug atm native** and **debug atm nmba**. These commands can be used to troubleshoot ATM switched virtual circuits (SVCs). The **debug atm nbma** and **debug atm native** commands are used to debug problems with Resource Reservation Protocol (RSVP) SVC creation and teardown. The **debug atm native** command can also be used to debug problems with SVCs created using static maps.

Benefits

The ATM SVC Troubleshooting Enhancements feature provides two debug commands that can be used to troubleshoot ATM SVCs that were created using static maps or RSVP.

Restrictions

The **debug atm nmba** command can be used only to debug RSVP SVCs. The **debug atm native** command can be used only to debug problems with RSVP SVCs or SVCs that were created using static maps.

Related Documents

- *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2
- *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2

Supported Platforms

- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7200 series
- Cisco 7500 series
- Cisco MC3810 series
- Universal Router Module (URM) for Cisco IGX 8400

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Supported Standards, MIBs, and RFCs

Standards

API Semantics for Native ATM Services, ATM Forum, February 1999

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

The tasks in this document assume that ATM SVCs or RSVP SVCs are already created.

Configuration Tasks

None.

Monitoring and Maintaining ATM SVCs

To monitor and maintain RSVP SVCs or ATM SVCs that were created using static maps, use the following commands in privileged EXEC mode:

Command	Purpose
Router# **debug atm native** {[**api**] | [**conn**] | [**error**] | [**filter**]}	Displays Native ATM API events.
Router# **debug atm nbma** [**api**]	Displays NBMA API events during the creation of RSVP SVCs.

Configuration Examples

None.

Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **debug atm native**
- **debug atm nbma**

DHCP Client on WAN Interfaces

Feature History for DHCP Client on WAN Interfaces

Release	Modification
12.2(8)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

This document describes the DHCP Client on WAN Interfaces feature in Cisco IOS Release 12.2(8)T and includes the following sections:

Feature Overview

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

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

Benefits

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

Restrictions

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

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

See the "Troubleshooting Tips" section of this document for more information.

Related Features and Technologies

- ATM
- DHCP Client

Related Documents

- *Cisco IOS IP Configuration Guide*, Release 12.2
- *Cisco IOS IP Command Reference, Vol 1 of 3: Addressing and Services*, Release 12.2
- *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2
- *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2

Supported Platforms

- Cisco 800 series
- Cisco 805
- Cisco 806
- Cisco 820
- Cisco 828
- Cisco 1720
- Cisco 1721
- Cisco 1750

- Cisco 1751
- Cisco 2420
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100
- Cisco 7200 series
- Cisco 7500 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Configuration Tasks

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

Troubleshooting Tips

- An ATM primary interface is always multipoint.
- An ATM subinterface can be multipoint or point-to-point.
- If you are using a point-to-point interface, the routing table determines when to send a packet to the interface and ATM map entries are not needed. Consequently, Inverse ARP, which builds ATM map entries, is not needed.
- If you are using a multipoint interface you must use Inverse ARP to discover the IP address of the other side of the connection.
- You can specify Inverse ARP through the **protocol ip inarp** interface configuration command. You must use the aal5snap encapsulation type when using Inverse ARP because it is the only encapsulation type that supports Inverse ARP.

Configuration Examples

This section provides the following configuration examples:

- ATM Primary Interface (Multipoint) Using aal5snap Encapsulation and Inverse ARP Example
- ATM Point-to-Point Subinterface Using aa15snap Encapsulation Example
- ATM Point-to-Point Subinterface Using aa15nlpid Encapsulation Example
- ATM Point-to-Point Subinterface Using aa15mux PPP Encapsulation Example

ATM Primary Interface (Multipoint) Using aal5snap Encapsulation and Inverse ARP Example

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

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

ATM Point-to-Point Subinterface Using aa15snap Encapsulation Example

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

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

ATM Point-to-Point Subinterface Using aa15nlpid Encapsulation Example

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

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

ATM Point-to-Point Subinterface Using aa15mux PPP Encapsulation Example

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

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

Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **ip address dhcp**

Glossary

ATM—Asynchronous Transfer Mode.

DHCP—Dynamic Host Configuration Protocol.

INARP—Inverse ARP.

PPP—Point-to-Point Protocol.

PPPoA—Point-to-Point Protocol over ATM.

Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

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

Feature Specifications for Cisco Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

Feature History	
Release	**Modification**
12.3(4)XD	These features were introduced.
12.3(7)T	These features were integrated into Cisco IOS Release 12.3(7)T.
Supported Platforms	
Cisco 3660, Cisco 3745	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

This feature module includes the following sections:

Prerequisites for Cisco Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

The Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features require a Cisco 3660 or Cisco 3745 with the following components installed:

Table 6 Supported Network Modules

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

Restrictions for Cisco Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

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

  http://www-tac.cisco.com/Support_Library/field_alerts/fn25194.html
- Voice activity detection (VAD) and echo cancellation are disabled when lossless compression is enabled.
- Lossless compression R1 is supported for VoATM calls with AAL2 and subcell multiplexing. VoIP calls are not supported at this time.

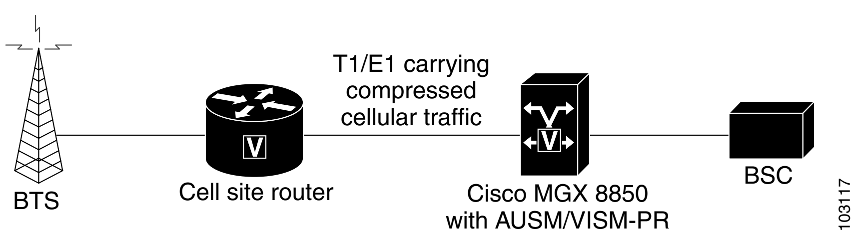
- ATM cell switching is limited to a maximum of 25 connections per AIM-ATM.
- Do not configure more than 29 LLCC channels per NM-HDV module. Configuring more than 29 LLCC channels can cause unreliable operation.
- J1 controller is not supported.
- Traffic policing is not supported.
- For Cisco 3660 routers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

  Using these slot combinations can result in packet loss.

Information About Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

The Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features work together to groom and compress T1 and E1 traffic between cell sites and a mobile central office. These features require a Cisco 3660 or Cisco 3745 router to be installed at the base transceiver station (BTS). This cell site router performs ATM switching and compression of cell site traffic for transport to the base station controller (BSC). A Cisco MGX 8850 with AUSM and VISM-PR terminates the T1/E1 lines that carry lossless compression codec (LLCC) traffic, converting the traffic back to PCM before passing it to the BSC. Figure 9 shows a sample topology that makes use of the Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features.

Figure 9 Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source Features



Lossless Compression Codec on NM-HDV

The Lossless Compression R1 feature introduces a new compression technique in DSP firmware and the VISM card— the lossless compression codec (LLCC). LLCC operates in a similar fashion to the existing clear channel codec: the decoded 64kbps PCM stream is a bit-exact replica of the PCM stream provided on the TDM side of the encoding DSP. However, rather than simply packetizing the PCM stream, the LLCC encoder applies a lossless data compression scheme. This results in a net reduction in the data transmission rate, yielding a reduction in the packet transmission rate.

ATM Cell Switching on AIM-ATM and AIM-ATM-VOICE-30

The Cisco ATM Cell Switching feature enables the router to perform cell switching between two ATM connections on AIM-ATM and AIM-ATM-VOICE-30 cards, giving the router the ability to receive ATM traffic from the BTS and backhaul it to the mobile central office.

BITS Clocking on the Cisco 3660 and Cisco 3745

BITS (Building Integrated Timing Supply) network clocking enables a Cisco 3660 or Cisco 3745 router to derive network timing from the central office. BITS must be configured on the cell site router to support this feature.

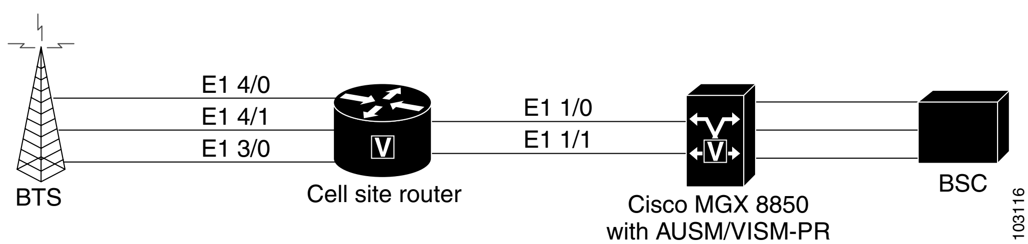
How to Configure Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

The procedures for configuring the Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features require the following tasks:

- Configuring the Cell Site Router for BITS Clocking, page 155
- Configuring ATM Cell Switching, page 156
- Configuring the Lossless Compression Codec, page 158
- Disabling Connection Admission Control, page 161

The instructions that follow refer to the sample configuration shown in Figure 10. With this configuration, the cell site router supports three E1 connections to the BTS. Compressed cellular traffic is transported to the BSC (by way of the Cisco MGX 8850) over the E1 1/0 and E1 1/1 interfaces. Additionally, BITS clocking is derived from E1 1/1.

Figure 10 Sample Configuration



Configuring the Cell Site Router for BITS Clocking

BITS clocking enables the router at a cell site to derive timing from the mobile central office. BITS clocking ensures that data flows to a single network clock source, preventing mismatches and data slips in traffic between the BTS and the BSC. The procedure that follows configures the AIM to receive BITS clocking from E1 1/1 controller.

Summary Steps

1. **enable**
2. **configure terminal**
3. **network-clock-participate** *slot number*
4. **network-clock-select** *priority slot number*
5. **controller e1** *slot/port*
6. **clock source {line [primary | bits] | internal}**

Detailed Steps

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 1`	Allows the network module in the specified slot to use the network clock for its timing.
Step 4	**network-clock-select** *priority slot number* **Example:** `Router(config)# network-clock-select 1 E1 1/1`	Specifies a port to be used as a timing source for the network clock, and the priority level for the use of that port. The source that is given the highest priority is used first; if it becomes unavailable, the source with the second-highest priority is used, and so forth.
Step 5	**controller t1 | e1** *slot/port* **Example:** `Router(config)# controller e1 1/1`	Enters controller configuration mode for the selected T1 or E1.
Step 6	**clock source {line [primary | bits] | internal}** **Example:** `Router(config-controller)# clock source line bits`	Specifies that the clock is generated from the T1 or E1 BITS source.

Configuring ATM Cell Switching

The procedure that follows configures the cell site router to switch ATM traffic with the Cisco MGX 8850 at the BSC. This procedure configures ATM switching between E1 3/0 and E1 1/0, using the AIM installed in Slot 1.

Summary Steps

1. **enable**
2. **configure terminal**
3. **network-clock-participate slot** *number*
4. **network-clock-participate slot** *number*
5. **network-clock-participate aim** *number*
6. **controller t1 | e1** *slot/port*
7. **mode atm aim** *aim-slot*
8. **controller t1 | e1** *slot/port*
9. **mode atm aim** *aim-slot*
10. **interface atm** *interface-number/subinterface-number*
11. **pvc** *vpi/vci* **l2transport**
12. **interface atm** *interface-number/subinterface-number*
13. **pvc** *vpi/vci* **l2transport**
14. **connect** *id* **atm** *slot/port-1* **atm** *slot/port-2*

Detailed Steps

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 1`	Enables the network module in the specified slot to use the network clock for its timing.
Step 4	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 3`	Enables the network module in the specified slot to use the network clock for its timing.

	Command or Action	Purpose
Step 5	**network-clock-participate aim** *number* **Example:** `Router(config)# network-clock-participate aim 0`	Specifies that the AIM in Slot 0 will derive clocking from the network source.
Step 6	**controller t1 | e1** *slot/port* **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode for the selected T1 or E1.
Step 7	**mode atm aim** *aim-slot* **Example::** `Router(config-controller)# mode atm aim 0`	Sets the mode of the T1 or E1 controller in AIM Slot 0.
Step 8	**controller t1 | e1** *slot/port* **Example:** `Router(config)# controller e1 3/0`	Enters controller configuration mode for the selected T1 or E1.
Step 9	**mode atm aim** *aim-slot* **Example:** `Router(config-controller)# mode atm aim 0`	Sets the mode of the T1 or E1 controller in AIM Slot 0.
Step 10	**interface atm** *interface-number/subinterface-number* **Example:** `Router(config) # interface atm 1/0`	Enters configuration mode for the selected ATM interface.
Step 11	**pvc** *vpi/vci* **l2transport** **Example:** `Router(config-if)# pvc 10/110 l2transport`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies that the PVC is switched, not terminated.
Step 12	**interface atm** *interface-number/subinterface-number* **Example:** `Router (config) # interface atm 3/0`	Enters configuration mode for the selected ATM interface.
Step 13	**pvc** *vpi/vci* **l2transport** **Example:** `Router(config-if)# pvc 30/130 l2transport`	Creates a PVC for the VPI and VCI and specifies that the PVC is switched.
Step 14	**connect** *id* **atm** *slot/port-1* **atm** *slot/port-2* `Router(config)# connect Switched-Conn atm 1/0 10/110 atm 3/0 30/130`	Defines connections between T1 or E1 controller ports and the ATM interface.

Configuring the Lossless Compression Codec

The procedure that follows configures an LLCC voice channel on E1 4/0 and sends it over the ATM network using E1 1/0 and the AIM installed in Slot 1.

Summary Steps

1. **enable**
2. **configure terminal**
3. **network-clock-participate slot** *number*
4. **network-clock-participate slot** *number*
5. **network-clock-participate aim** *number*
6. **voice service {pots | voatm | vofr | voip}**
7. **session protocol aal2**
8. **subcell-mux**
9. **codec aal2-profile custom** *profile-number* **codec**
10. **controller t1 | e1** *slot/port*
11. **mode atm aim** *aim-slot*
12. **controller t1 | e1** *slot/port*
13. **ds0-group** *ds0-group-number* **timeslots** *timeslot-list* **type** *signaling method*
14. **interface atm** *interface-number/subinterface-number*
15. **pvc** *vpi/vci*
16. **vbr-rt** *peak-rate average-rate burst*
17. **encapsulation aal2**
18. **dial-peer voice** *tag* **voatm**
19. **destination-pattern** *string*
20. **session protocol aal2-trunk**
21. **session target** *interface* **pvc** *vpi/vci*
22. **signal-type cas | cept | ext-signal | transparent**
23. **codec aal2-profile custom** *profile-number* **codec**
24. **voice-port** {*slot-number/subunit-number/port* | *slot/port*:*ds0-group-no*}
25. **playout-delay {fax | maximum | nominal}** *milliseconds*
26. **connection {plar | tie-line | plar-opx}** *digits* | **{trunk** *digits* **[answer-mode]}**

Detailed Steps

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 1`	Enables the network module in the specified slot to use the network clock for its timing.
Step 4	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 4`	Enables the network module in the specified slot to use the network clock for its timing.
Step 5	**network-clock-participate aim** *number* **Example:** `Router(config)# network-clock-participate aim 0`	Specifies that the AIM in Slot 0 will derive clocking from the network source.
Step 6	**voice service {pots | voatm | vofr | voip}** **Example:** `Router(config)# voice service voatm`	Enters voice service configuration mode and specifies VoATM as the encapsulation type.
Step 7	**session protocol aal2** **Example:** `Router(config-voi-serv)# session protocol aal2`	Enters voice-service-session configuration mode and specifies ATM adaptation layer 2 (AAL2) trunking.
Step 8	**subcell-mux** **Example:** `Router(conf-voi-serv-sess)# subcell-mux`	Enables AAL2 common part sublayer (CPS) subcell multiplexing.
Step 9	**codec aal2-profile custom** *profile-number* **codec** **Example:** `Router# codec aal2-profile custom 51 0 0 llcc 40 0 15`	Sets the codec profile for the DSP on a per-call basis and specifies the lossless compression codec.
Step 10	**controller t1 | e1** *slot/port* **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode for the selected T1 or E1.

	Command or Action	Purpose
Step 11	**mode atm aim** *aim-slot* **Example:** `Router(config-controller)# mode atm aim 0`	Sets the mode of the T1 or E1 controller in AIM Slot 0.
Step 12	**controller t1 | e1** *slot/port* **Example:** `Router(config)# controller e1 4/0`	Enters controller configuration mode for the selected T1 or E1.
Step 13	**ds0-group** *ds0-group-number* **timeslots** *timeslot-list* **type** *signaling method* **Example:** `Router(config-controller)#` **ds0-group 0 timeslots 1 type ext-sig**	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type used by the router.
Step 14	**interface atm** *interface-number/subinterface-number* **Example:** `Router(config) #` **interface atm 1/0**	Enters configuration mode for the selected ATM interface.
Step 15	**pvc** *vpi/vci* **Example:** `Router(config-if-atm)#` **pvc 10/110**	Enters configuration mode for the selected PVC.
Step 16	**vbr-rt** *peak-rate average-rate burst* **Example:** `Router(config-if-atm-pvc)#` **vbr-rt 1920 1920 255**	Configures real-time variable bit rate (VBR) for VoATM voice connections.
Step 17	**encapsulation aal2** **Example:** `Router(config-if-atm-pvc)#` **encapsulation aal2**	Configures the encapsulation type for the ATM virtual circuit.
Step 18	**dial-peer voice** *tag* **voatm** **Example:** `Router(config)#` **dial-peer voice 1001 voatm**	Defines a dial-peer and specifies the method of voice encapsulation as VoATM.
Step 19	**destination-pattern** *string* **Example:** `Router(config-dial-peer)#` **destination-pattern 1001**	Specifies the prefix to be used by the dial peer.
Step 20	**session protocol aal2-trunk** **Example:** `Router(config-dial-peer)#` **session protocol aal2-trunk**	Specifies the dial peer uses AAL2 nonswitched trunk session protocol.

	Command or Action	Purpose
Step 21	**session target** *interface* **pvc** *vpi/vci* **Example:** `Router(config-dial-peer)#` **`session target atm 1/0 pvc 10/100 9`**	Specifies the network-specific address for the VoATM dial peer.
Step 22	**signal-type cas | cept | ext-signal | transparent** **Example:** `Router(config-dial-peer)#` **`signal-type ext-signal`**	Specifies that external signaling is used when connecting to the dial peer. The DSP does not generate any signaling frames.
Step 23	**codec aal2-profile custom** *profile-number* **codec** **Example:** `Router(config-dial-peer)#` **`codec aal2-profile custom 51 llcc`**	Sets the codec profile for the DSP on a per-call basis and specifies the lossless compression codec.
Step 24	**voice-port** {*slot-number/subunit-number/port* | *slot/port:ds0-group-no*} **Example:** `Router(config)#` **`voice-port 2/0:0`**	Enters voice-port configuration mode.
Step 25	**playout-delay {fax | maximum | nominal}** *milliseconds* **Example:** `Router(config-voice-port)#` **`playout-delay nominal 25`**	Tunes the playout buffer to accommodate packet jitter caused by switches in the WAN. The **nominal** keyword specifies the initial (and minimum allowed) delay time that the DSP inserts before playing out voice packets, in milliseconds.
Step 26	**connection {plar | tie-line | plar-opx}** *digits* | **{trunk** *digits* **[answer-mode]}** **Example:** `Router(config-voice-port)#` **`connection trunk 1001`**	Associates this voice-port to destination-pattern 1001.

Note To ensure that the voice-port configuration takes affect, issue the **shutdown** command, followed by **no shutdown** to enable it again.

Disabling Connection Admission Control

Connection admission control (CAC) is a set of actions taken by each ATM switch during connection setup to determine whether the requested QoS will violate the QoS guarantees for established connections. CAC reserves bandwidth for voice calls, however, the bandwidth required when LLCC is used is dynamic and usually less than what is generally reserved by CAC. Disabling CAC may help in better utilization of bandwidth when LLCC is used. The procedure that follows disables CAC.

Summary Steps

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number/subinterface-number*
4. **pvc** *vpi/vci*
5. **cac_off**

Detailed Steps

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**`configure terminal`** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**`interface atm`** *`interface-number/subinterface-number`* **Example:** `Router(config) #` **`interface atm 1/0`**	Enters configuration mode for the selected ATM interface.
Step 4	**`pvc`** *`vpi/vci`* **Example:** `Router(config-if-atm)#` **`pvc 10/110`**	Enters configuration mode for the selected PVC.
Step 5	**`cac_off`** **Example:** `Router# (config-if-atm-vc)#` **`cac_off`**	Disables call admission control.

Verifying Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source Configuration

This section provides a set of **show** commands you can use to verify the configuration of the Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features. It includes the following commands:

- show connection all
- show voice dsp
- show voice call port-id
- show voice trunk supervisory summary
- show interfaces

show connection all

The following example shows output from the **show connection all** command. In this example, Switched-Conn is a cell-switched connection established between PVC 10/110 and PVC 30/130, which are configured under ATM1/0 and ATM3/0 respectively.

```
Router# show connection all
ID    Name              Segment 1             Segment 2           State
========================================================================
3     V-100-700         E1 1/0(VOICE) 00      DSP 07/00/00        UP
4     V-120-700         E1 1/2(VOICE) 00      DSP 07/00/00        UP
5     Switched-Conn     ATM1/0 10/110         ATM3/0 30/130       UP
```

The **show connection all** command displays the state of Switched-Conn. If it is in the UP state, then it means the ATM cell switching connection is operational.

show voice dsp

The following example shows output from the **show voice dsp** command:

```
Router# show voice dsp
DSP  DSP              DSPWARE CURR  BOOT                             PAK   TX/RX
TYPE NUM CH CODEC     VERSION STATE STATE   RST AI VOICEPORT TS ABORT PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ==========
C549 000 04 llcc     4.3.392 busy  idle         0 4/0:0     04     0 1752/1752
```

The **show voice dsp** command shows if the LLCC codec has been applied to the voice port. Additionally, the TX/RX COUNT indicates if packet exchange is occurring. If LLCC is operational, then TX/RX COUNT will display similar values.

show voice call *port-id*

The **show voice call** command gives detailed information about the lossless compression codec. The following example shows output from the **show voice call** command:

Note The **show voice call** command has a limitation that causes it to display invalid values. To ensure that accurate values are reported, invoke this command twice and look at the second output.

```
Router# show voice call 4/0:0
4/0:0 1
      vtsp level 0 state = S_CONNECTvpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP

lossless compression summary:
    average compression ratio since reset       = 50
    current compression ratio                   = 50
    max buffer size (ms)                        = 41
    nominal buffer size (ms)                    = 25
    current buffer size (ms)                    = 26
    total encoder input frame count             = 5534
    total encoder output frame count            = 2767
    encoded tx front-end compressed frame count = 2767
    encoded tx back-end compressed frame count  = 0
    encoded tx frame count (no compression)     = 0
    underflow error count                       = 0
    overflow error count                        = 0
    decode error count                          = 0
    tx signalling frame count                   = 11
    rx signalling frame count                   = 10
    rx bad checksum frame count                 = 0
    rx good checksum frame count                = 2777
```

show voice trunk supervisory summary

The following example shows output from the **show voice trunk supervisory summary** command:

```
Router# show voice trunk supervisory summary
SLOW SCAN
4/0:0(1) : state : TRUNK_SC_CCS_CONNECT, master
```

show interfaces

The following example shows output from the **show interfaces** command:

```
Router# show interfaces atm1/0
ATM1/0 is up, line protocol is up
  Hardware is ATM AIM E1
  MTU 4470 bytes, sub MTU 4470, BW 1920 Kbit, DLY 20000 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Encapsulation(s): AAL5
  255 maximum active VCs, 256 VCs per VP, 0 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Per VC Queueing
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Additional References

For additional information related to the Cisco Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source feature, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring voice features	Cisco IOS Voice Configuration Library, Release 12.3
Configuring ATM advanced integration modules	AIM-ATM and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series
Configuring high-density voice network modules	Digital E1 Packet Voice Trunk Network Module Interfaces

Standards

Standards[1]	Title
No new standards are supported by this feature.	

1. Not all supported standards are listed.

MIBs

MIBs	MIBs Link
• No new MIBs are supported by this feature. • CISCO-VOICE-COMMON-DIAL-CONTROL-MIB was modified.	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[1]	Title
No new RFCs are supported by this feature.	

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **cac_off**
- **clock source (T1/E1 controller)**
- **codec aal2-profile**
- **connect (atm)**

AAL1 CES on AIM-ATM

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

Feature Specifications for the AAL1 CES on AIM-ATM Feature

Feature History	
Release	**Modification**
12.3(8)T	This feature was introduced.
Supported Platforms	
Cisco 3660, Cisco 3745	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

This feature module includes the following sections:

Prerequisites for the AAL1 CES on AIM-ATM Feature

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

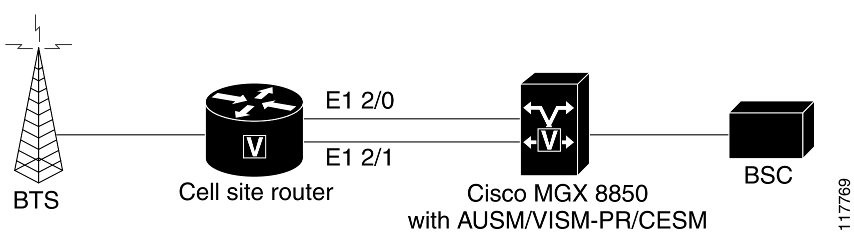
Restrictions for the AAL1 CES on AIM-ATM Feature

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

Configuring AAL1 CES on AIM-ATM

The sample configuration in this section is based on Figure 11.

Figure 11 AAL1 CES on AIM-ATM Sample Configuration



Configuring AAL1 CES on AIM-ATM

Summary Steps

1. **enable**
2. **configure terminal**
3. **network-clock-participate slot** *number*
4. **network-clock-participate slot** *number*
5. **network-clock-participate aim** *number*
6. **controller t1 | e1** *slot/port*
7. **mode atm aim** *aim-slot*
8. **controller t1 | e1** *slot/port*
9. **tdm-group** *tdm-group-no* **timeslots** *timeslot-list*

10. **tdm-group** *tdm-group-no* **timeslots** *timeslot-list*
11. **interface atm** *interface-number*/*subinterface-number*
12. **pvc** *vpi*/*vci* **[ces]**
13. **ces-cdv** *time*
14. **exit**
15. **pvc** *vpi*/*vci* **ces**
16. **ces-cdv** *time*
17. **exit**
18. **exit**
19. **connect** *connection-name* **atm** *slot/port* [*name of PVC/SVC*|*vpi*/*vci*] **E1** *slot/port TDM-group-number*
20. **connect** *connection-name* **atm** *slot/port* [*name of PVC/SVC*|*vpi*/*vci*] **E1** *slot/port TDM-group-number*

Detailed Steps

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

	Command or Action	Purpose
Step 7	**mode atm aim** *aim-slot* **Example::** `Router(config-controller)# mode atm aim 1`	Sets the mode of the T1 or E1 controller in AIM Slot 1.
Step 8	**controller t1 | e1** *slot/port* **Example:** `Router(config)# controller e1 2/0`	Enters controller configuration mode for the selected T1 or E1.
Step 9	**tdm-group** *tdm-group-no* **timeslots** *timeslot-list* **Example:** `Router(config-controller)# tdm-group 1 timeslots 1`	Configure a TDM channel group for the T1 or E1 interface. *tdm-group-no* is a value from 0 to 23 for T1 and from 0 to 30 for E1; it identifies the group. *timeslot-list* is a single number, numbers separated by commas, or a pair of numbers separated by a hyphen to indicate a range of timeslots. The valid range is from 1 to 24 for T1. For E1, the range is from 1 to 31.
Step 10	**tdm-group** *tdm-group-no* **timeslots** *timeslot-list* **Example:** `Router(config-controller)# tdm-group 2 timeslots 17-31`	Configure a TDM channel group for the T1 or E1 interface.
Step 11	**interface atm** *interface-number/subinterface-number* **Example:** `Router(config) # interface atm 1/0`	Enters configuration mode for the selected ATM interface.
Step 12	**pvc** *vpi/vci* **[ces]** **Example:** `Router(config-if)# pvc 4/44 ces`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies CES encapsulation. Enters interface-ATM-VC configuration mode.
Step 13	**ces-cdv** *time* **Example:** `Router(config-if-ces-vc)# ces-cdv 500`	Configures the cell delay variation (CDV). The configuration command has the format **ces-cdv** `<time>` where the time is the maximum tolerable cell arrival jitter with a range of 1 to 65535 microseconds.
Step 14	**exit** **Example:** `Router(config-if-ces-vc)# exit`	Exits back to interface configuration mode.
Step 15	**pvc** *vpi/vci* **ces** **Example:** `Router(config-if)# pvc 8/88 ces`	Creates a second PVC and enters interface-ATM-VC configuration mode.
Step 16	**ces-cdv** *time* **Example:** `Router(config-if-ces-vc)# ces-cdv 1000`	Configures the CDV for 1000 microseconds.

	Command or Action	Purpose
Step 17	**exit** **Example:** `Router(config-if-ces-vc)# exit`	Exits back to interface configuration mode.
Step 18	**exit** **Example:** `Router(config-if)# exit`	Exits back to configuration mode.
Step 19	**connect** *connection-name* **atm** *slot/port* [*name of PVC/SVC*|*vpi/vci*] **T1** *slot/port TDM-group-number* **Example:** `Router(config)# connect alpha ATM 1/0 4/44 E1 2/0 1`	Defines connections between T1 or E1 controller ports and the ATM interface.
Step 20	**connect** *connection-name* **atm** *slot/port* [*name of PVC/SVC*|*vpi/vci*] **T1** *slot/port TDM-group-number* **Example:** `Router(config)# connect alpha ATM 1/0 8/88 E1 2/0 2`	Defines connections between T1 or E1 controller ports and the ATM interface.

Configuring IMA Groups

Summary Steps

1. **enable**
2. **configure terminal**
3. **network-clock-participate slot** *number*
4. **network-clock-participate aim** *number*
5. **controller t1 | e1** *slot/port*
6. **mode atm aim** *aim-slot*
7. **interface atm** *interface-number/subinterface-number*
8. **ima-group** *group-number*
9. **exit**
10. Repeat Step 7 through Step 9.
11. **interface atm** *slot*/**ima***group-number*
12. **pvc** *vpi/vci* **[ces]**
13. **partial-fill** *octet*
14. **exit**
15. **pvc** *vpi/vci* **[ces]**
16. **ces-cdv** *time*
17. **exit**
18. **exit**

19. **connect** *connection-name* **atm** *slot/port* [*name of PVC/SVC*|*vpi/vci*] **E1** *slot/port* *TDM-group-number*

Detailed Steps

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**network-clock-participate slot** *number* **Example:** `Router(config)# network-clock-participate slot 2`	Enables the network module in the specified slot to use the network clock for its timing.
Step 4	**network-clock-participate aim** *number* **Example:** `Router(config)# network-clock-participate aim 0`	Specifies that the AIM in Slot 0 will derive clocking from the network source.
Step 5	**controller t1 | e1** *slot/port* **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode for the selected T1 or E1.
Step 6	**mode atm aim** *aim-slot* **Example::** `Router(config-controller)# mode atm aim 1`	Sets the mode of the T1 or E1 controller in AIM Slot 1.
Step 7	**interface atm** *interface-number/subinterface-number* **Example:** `Router(config)# interface atm 2/1`	Enters configuration mode for the selected ATM interface.
Step 8	**ima-group** *group-number* **Example:** `Router(config-if)# ima-group 0`	Specifies that the link is included in an IMA group. Enter an IMA group number from 0 to 3.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 10	Repeat Step 7 through Step 9 to add ATM 2/3 to IMA group 0.	

	Command or Action	Purpose
Step 11	**interface atm** *slot*/**ima***group-number* **Example:** `Router(config)# interface atm 0/ima0`	Enter interface configuration mode for the IMA group.
Step 12	**pvc** *vpi/vci* **[ces]** **Example:** `Router(config-if)# pvc 5/55 ces`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies CES encapsulation. Enters interface-ATM-VC configuration mode.
Step 13	**partial-fill** *octet* **Example:** `Router(config-if-ces-vc)# partial-fill 35`	Configures the number of AAL1 user octets per cell for CES. The range of values is 1–46 for T1 and 20–47 for E1. **Note** Partial fill and CDV cannot be modified under a CES PVC that is part of any connection. Do not establish the connection until after you enter the partial-fill and CDV values.
Step 14	**exit** **Example:** `Router(config-if-ces-vc)# exit`	Exits back to interface configuration mode.
Step 15	**pvc** *vpi/vci* **[ces]** **Example:** `Router(config-if)# pvc 6/66 ces`	Creates a PVC for the virtual path identifier (VPI) and virtual channel identifier (VCI) and specifies CES encapsulation. Enters interface-ATM-VC configuration mode.
Step 16	**ces-cdv** *time* **Example:** `Router(config-if-ces-vc)# ces-cdv 1000`	Configures the CDV for 1000 microseconds.
Step 17	**exit** **Example:** `Router(config-if-ces-vc)# exit`	Exits back to interface configuration mode.
Step 18	**exit** **Example:** `Router(config-if)# exit`	Exits back to configuration mode.
Step 19	**connect** *connection-name* **atm** *slot/port* [*name of PVC/SVC*|*vpi/vci*] **E1** *slot/port TDM-group-number* **Example:** `Router(config)# connect alpha-IMA atm0/ima0 5/55 E1 2/0 1`	Establishes the connection between the T1 or E1 controller ports and the IMA group.

Sample Configuration for AAL1 CES on AIM-ATM

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

```
network-clock-participate slot 1
network-clock-participate slot 2
network-clock-participate aim 1

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

Note TDM-group defined for 1 timeslot.

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

Note TDM-group defined for 15 timeslots.

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

Note Default CDV value set to 5 microseconds.

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

Note Default CDV value set to 1 second.

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

Note CES connections for TDM-AAL1 CES PVCs.

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

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

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

Note Default cdv value set to 5 microseconds.

```
 partial-fill 35
```

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

```
 pvc 6/66 ces
  ces-cdv 1000

connect alpha-IMA atm0/ima0 5/55 E1 2/0 1
```

Verifying the AAL1 CES on AIM-ATM Feature

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

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

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

```
Router#show connection name 1ds0

Connection: 4 - 1ds0
 Current State: UP
 Segment 1:  ATM2/2 pvc 4/44
 Segment 2:  E1 2/0 01
  TDM timeslots in use: 1 (1 total)
 Internal Switching Elements: VPD
 CES-CDV: 5000 usec, Partial Fill: 0 bytes
```

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

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

Note Only synchronous clocking is supported.

Additional References

For additional information related to the AAL1 CES on AIM-ATM feature, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring voice features	Cisco IOS Voice Configuration Library, Release 12.3
Configuring ATM advanced integration modules	AIM-ATM and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series
Configuring high-density voice network modules	Digital E1 Packet Voice Trunk Network Module Interfaces

Standards

Standards	Title
No new standards are supported by this feature.	

MIBs

MIBs	MIBs Link
No new MIBs are supported 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[1]	Title
No new RFCs are supported by this feature.	

1. Not all supported RFCs are listed.

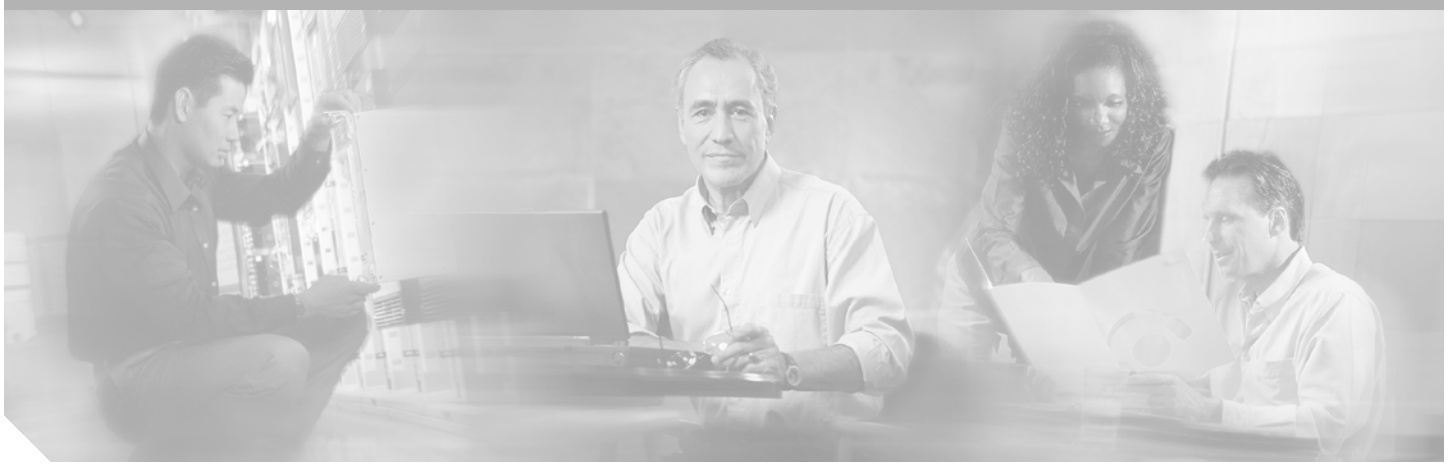
Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **pvc**



Part 2: LAN ATM

LAN Emulation Overview

This part consists of the following:

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.

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

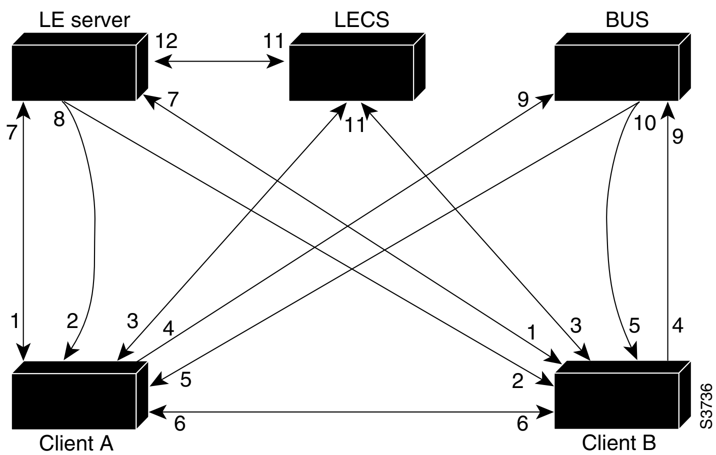
Note ELAN names must be unique on an interface. If two interfaces participate in LANE, the second interface may be in a different switch cloud.

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

Figure 12 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 12 LANE VCC Types



1–7	Control direct	4–9	Multicast send
2–8	Control distribute	5–10	Multicast forward
3–11	Configure direct (client)	6–6	Data direct
		11–12	Configure direct (server)

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 13 illustrates a scenario in which one ELAN is set up on the switch and routers. Figure 14 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.

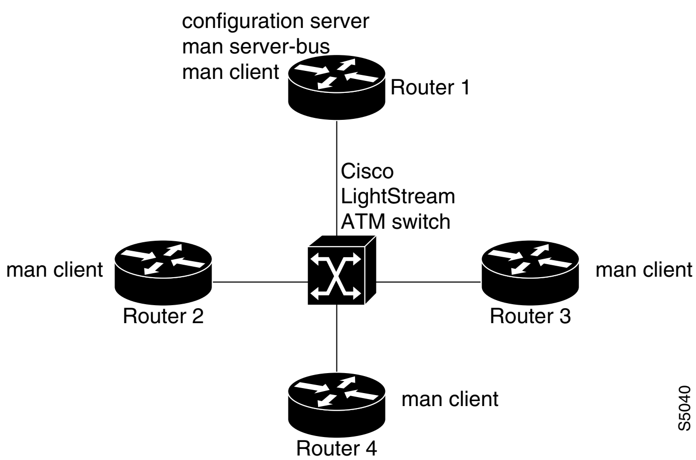
Single ELAN Scenario

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 13 illustrates this single ELAN configured across several routers.

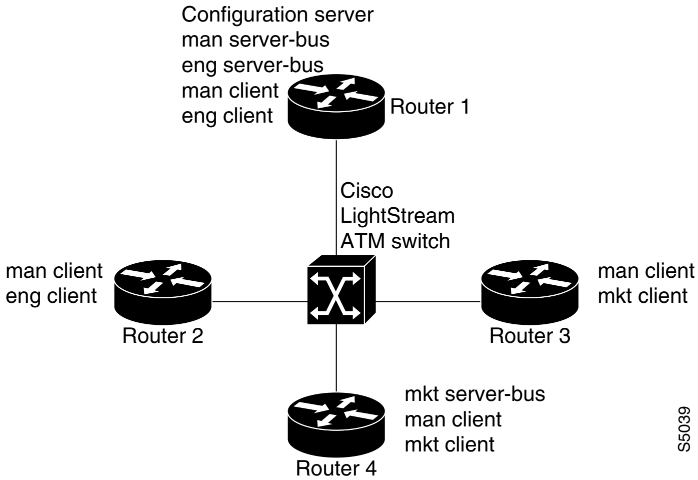
Figure 13 Single ELAN Configured on Several Routers



Multiple ELAN Scenario

In the multiple LAN scenario, the same switch and routers are used, but multiple ELANs are configured. See Figure 14.

Figure 14 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.

SNMP Trap Support for the Virtual Switch Interface Master MIB

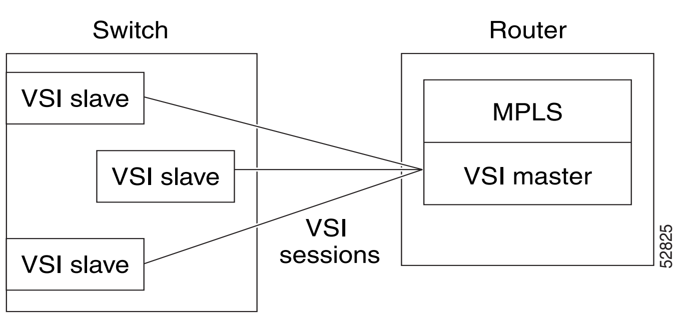
This feature module explains how to use the virtual switch interface (VSI) Master MIB to monitor and manage ATM switches that are connected to routers through the virtual switch interface.

This document includes the following major sections:

Feature Overview

The VSI master is a software module that resides on a router. The VSI master enables an application to control an ATM switch that is connected to the router. The VSI protocol runs between the VSI master and a VSI slave. The VSI master can communicate with more than one slave across a control interface that connects the router to the switch. Each master/slave connection is called a VSI session. Figure 15 illustrates VSI sessions between a VSI master and slaves.

Figure 15 VSI Master and VSI Slaves



Overview of the SNMP Trap Support for the VSI Master MIB

The VSI Master MIB allows you to manage and monitor the activities of the VSI components, including controllers, sessions, logical interfaces, and cross-connects. The MIB provides notifications in the form of traps when any of the VSI components change operational state, violate configured thresholds, or are added or removed.

The MIB allows you to specify which VSI components can send traps. To enable the traps for certain VSI components, you can use the MIB objects or Cisco IOS commands. See the section "Enabling Traps" for more information.

VSI Components You Can Monitor with the VSI Master MIB

The VSI Master MIB allows you to monitor the operation of the switch. It also displays the results of the operations. Specifically, the VSI Master MIB allows you to monitor:

- Connections between the router and the controlled switch.
- The status of the interfaces in the switch
- Virtual circuits (VCs) that are maintained across the interfaces.

MIB Traps

The VSI Master MIB allows you to enable traps on the following components:

Controllers—When VSI controllers are added or deleted

VSI sessions—When VSI sessions are established or disconnected

Logical interfaces—When logical interfaces become active or fail.

Cross-connects—When a cross-connect cannot be established.

Virtual circuits—When cross-connect resource thresholds are below configured thresholds.

MIB Objects

The following is a partial list of the supported MIB objects.

Controllers

You can obtain the following information about the controller:

- Controller identifier
- Number of cross-connects maintained in the switch
- Protocol version
- Controller interface index
- Slave interface identifiers
- Controller IP address

Sessions

You can obtain the following information about the VSI sessions:

- Virtual path identifiers (VPIs) for session connections
- Virtual circuit identifiers (VCIs) for the sessions
- Switch identifier
- Switch name
- Session state
- Protocol session monitoring

Logical Interfaces

Logical interfaces represent external interfaces that are available for connections. When you pair two external interfaces (represented by two logical interfaces), they provide a physical path through the switch. These physical paths support cross-connects. You can gather the following information about each logical interface:

- Interface name
- Operational state
- Administrative state
- Operational statistics
- Cross-connect usage
- Cross-connect availability
- Cross-connect capacity
- Interface capabilities
- VC ranges
- Interface index
- IP address

Cross-Connects

Cross-connects are virtual links across two interfaces. The participating interfaces that support these links are listed in the MIB’s vsiLogicalIfTable entries. You can gather the following information about the cross-connects:

- Interface associations
- State
- Identifiers
- VPI/VCI identifiers for supporting interfaces

Restrictions

The VSI Master MIB is for ATM-LSRs running Multiprotocol Label Switching (MPLS).

Related Documents

See the following documents for more information:

- *Virtual Switch Interface Master MIB*

http://www.cisco.com/public/mibs/v2/CISCO-VSIMASTER-MIB.my

- *Multiprotocol Label Switching Overview*

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagov.htm

- *BPX Installation and Configuration Guide,* Chapter 23, "Configuring BXM Virtual Switch Interfaces"

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/9_3/bpx/bpxi23.htm#xtocid120351

Supported Platforms

This feature is supported on the following routing platforms:

- Cisco 7200 series router
- Cisco MGX 8850 Route Processor Module (RPM)

You can use the following ATM switches to configure an ATM-LSR:

- Cisco BPX 8600, 8650, and 8680 switches
- MGX BXM cards

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

Virtual Switch Interface Master MIB

http://www.cisco.com/public/mibs/v2/CISCO-VSIMASTER-MIB.my

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on Cisco Connection Online (CCO) at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Memory Requirements

- The VSI Master MIB requires 75K of space.

- The runtime dynamic random-access memory (DRAM) is approximately 5K times the number of logical/slave interfaces the VSI controller manages.

Performance

The VSI cross-connect error messages can be invoked hundreds of times every second. To prevent a performance impact on the label switch controller (LSC), enable rate-limiting to control the amount of traffic that passes into or out of an interface.

Configuration Tasks

See the following sections for configuration tasks for the VSI Master MIB feature. Each task in the list indicates whether the task is optional or required.

- Enabling the SNMP Agent (required)
- Verifying That the SNMP Agent Has Been Enabled (optional)
- Enabling Traps (required)
- Setting Thresholds for Cross-Connects (optional)

Enabling the SNMP Agent

The SNMP agent for the VSI Master MIB is disabled by default. To enable the SNMP agent, perform the following steps:

	Command	Purpose
Step 1	`prompt#` **`telnet 10.10.10.1`**	Accesses the router through a Telnet session.
Step 2	`router#` **`enable`**	Enters the privileged mode.
Step 3	`router#` **`show running-configuration`**	Displays the running configuration to see if the SNMP agent is already running. If no SNMP information is present, continue with the steps below. If any SNMP commands are listed, you can modify them or leave them as they are.
Step 4	`router#` **`configure terminal`**	Enters the configuration mode.
Step 5	`router(config)#` **`snmp-server community xxxxxx RO`**	Enables the read-only community string, where *xxxxxx* is the read-only community string
Step 6	`router(config)#` **`exit`**	Exits the configuration mode and returns to the main prompt.
Step 7	`router#` **`write memory`**	Writes the modified configuration to nonvolatile memory (NVRAM) so that the settings stay permanently.

Verifying That the SNMP Agent Has Been Enabled

To verify that the SNMP agent has been enabled, perform the following steps:

Step 1 Access the router through a Telnet session:

```
prompt# telnet 10.10.10.1
```

Step 2 Enter the privileged mode:

```
router# enable
```

Step 3 Display the running configuration and look for SNMP information:

```
router# show running-configuration
...
...
snmp-server community public RO
```

If you see any “snmp-server” statements, SNMP has been enabled on the router.

Enabling Traps

SNMP notifications can be sent as traps or inform requests. A trap is an unsolicited message sent by an SNMP agent to an SNMP manager, indicating that some event has occurred. You can enable SNMP traps for the VSI Master MIB through the command line interface (CLI) or through an SNMP MIB object. The following sections explain these options.

Using Commands to Enable the VSI Master MIB traps

To enable SNMP traps, use the **snmp-server enable traps** command. An SNMP agent can be configured to send traps when one of the VSI Master MIB objects changes. To enable VSI Master MIB traps to be sent from the agent to the manager, perform the following tasks in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`snmp-server enable traps vsimaster`**	Enables the router to send VSI Master MIB traps.
Step 2	`Router(config)#` **`snmp-server host`** ***`host community-string`*** **`vsimaster`**	Specifies the recipient of the trap message

Table 7 lists the CLI commands for enabling traps of specific VSI components.

Table 7 CLI Commands that Control the Type of Traps You Receive

To Receive Traps About	Use This Command
All components	**snmp server enable traps vsimaster**
Controllers being added or deleted	**snmp server enable traps vsimaster controller**
Sessions that connect or disconnect	**snmp server enable traps vsimaster session**

To Receive Traps About	Use This Command
Logical interfaces that connect or disconnect	**snmp server enable traps vsimaster logical-interface**
Cross-connects that fail	**snmp server enable traps vsimaster cross-connect**

Using SNMP MIB Objects to Enable the VSI Master MIB Traps

You can also use MIB objects to specify which VSI components should send traps. To enable all VSI Master traps, use the vsiVSITrapEnable MIB object.

Controller Traps

To enable traps about the status of the controller, use the vsiControllerTrapEnable MIB object. Table 8 lists the MIB objects that are specific to the controller.

Table 8 Controller Traps

To Receive Traps When	Use This MIB Object
A controller is added	vsiControllerAdded
A controller is deleted	vsiControllerDeleted

VSI Session Traps

To enable traps about the status of the VSI sessions, use the vsiSessionTrapEnable MIB object. Table 9 lists the MIB objects that are specific to the VSI sessions.

Table 9 VSI Session Traps

To Receive Traps When	Use This MIB Object
A VSI session is established	vsiSessionUp
A VSI session is disconnected	vsiSessionDown

Logical Interaces

To enable traps about the status of the logical interfaces, use the vsiLogicalIfTrapEnable MIB object. Table 10 lists the MIB objects that are specific to the logical interfaces.

Table 10 Logical Interface Traps

To Receive Traps When	Use This MIB Object
A logical interface is active	vsiLogicalIfUp
A logical interface fails	vsiLogicalIfDown

Cross-connects

To enable traps about the status of the cross-connects, use the vsiXCTrapEnable MIB object. Table 11 lists the MIB objects that are specific to the cross-connects.

Table 11 Cross-connect Traps

To Receive Traps When	Use This MIB Object
A cross-connect cannot be established	vsiXCFailed
The LCN resources drop, possibly causing resource exhaustion.	vsiLcnExhaustionNotice

Setting Thresholds for Cross-Connects

When cross-connects on XtagATM interfaces are created or deleted, a counter keeps a tally of the available logical channel number (LCN) resources. If the LCN resources become too low, the MIB sends messages to alert you of the possibility of resource exhaustion.

You must first set the warning and alarm thresholds for the number of LCNs. To set the warning threshold, use the vsiAvailableChnlWarnThreshold MIB object. To set the alarm threshold, use the vsiAvailableChnlAlarmThreshold MIB object. The following list explains the usage guidelines of these MIB objects:

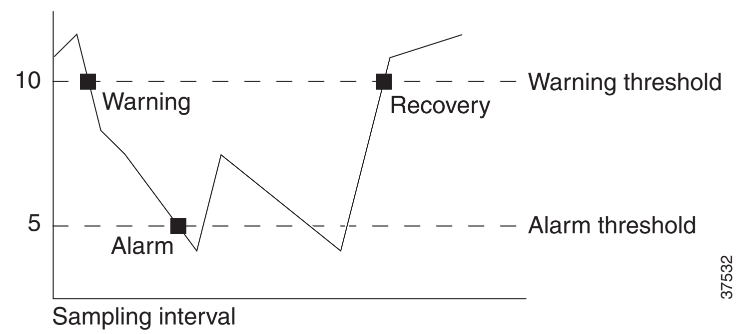
- The threshold range is 1 to 100.
- The warning threshold value must be greater than or equal to the value of the alarm threshold. Likewise, the alarm threshold value must be less than or equal to the value of the warning threshold.
- If you only set one threshold, the MIB automatically sets the other threshold value to the same value as the threshold value you set.
- By default, the threshold functionality is disabled.

The following list explains the conditions under which warnings, alarms, and other messages are sent. Figure 16 illustrates the thresholds.

- If the number of LCNs falls below the the warning threshold, a warning is sent. This message indicates that the potential for resource exhaustion is possible.
- If the number of LCNs falls below the alarm threshold, an alarm is generated. This message indicates that the potential for resource exhaustion is imminent. If resource exhaustion occurs, cross-connects cannot be set up.
- If the number of LCNs returns to above the warning threshold, a recovery message is generated. This message means that the potential for resource exhaustion no longer exists.
- If the number of LCNs never crosses any threshold during the polling period, a normal message is generated.

To prevent an overwhelming number of warnings or alarms from being generated durng a sampling period, only one warning or alarm is generated when the number of LCNs falls below the threshold. The number of LCNs must return to normal before another warning or alarm is generated.

Figure 16 Warning and Alarm Thresholds



Note If XtagATM interfaces share resources, the LCN does not represent the actual amount of available resources. For example, the interfaces XtagATM1 and XtagATM2 share resources. If a cross-connect is set up on XtagATM1but not on XtagATM2, XtagATM1 takes resources away from XtagATM2. When the VSI slave reports the available resources, it only reports on the resources for XtagATM1. The resources for XtagATM2 are not reported. This is because the VSI slave provides updates only when a cross-connect is set up or torn down or when the slave's resources are partitioned. Any interfaces that are not set up or torn down do not send updates. As a result, if XtagATM2 doesn't have enough resources in the resource pool, the problem does not get reported.

Configuration Examples

In the following example, the SNMP agent is enabled.

```
snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *publi*c.

```
snmp-server community public
```

In the following example, read-only access is granted for all objects to members of access list 4 that specify the *comaccess* community string. No other SNMP managers have access to any objects.

```
snmp-server community comaccess ro 4
```

In the following example VSI Master MIB traps are sent to the host cisco.com. The community string is restricted. The first line enables the router to send VSI Master MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server host** commands for the host cisco.com.

```
snmp-server enable traps vsi master
snmp-server host cisco.com restricted vsimaster
```

Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **snmp-server community**
- **snmp-server enable traps**
- **snmp-server host**

Glossary

agent—A process in the device that handles SNMP requests.

alarm—A message that is triggered when defined values cross a given threshold. For instance, you can specify the number of Ethernet collisions, plus a time interval, such as 1 second, and a threshold, such as 60 collisions. Given this scenario, an alarm is generated when the number of Ethernet collisions exceeds 60 in 1 second.

event—The action that is triggered as result of an alarm. Alarms and events are logically connected. For example, when the number of collisions on an Ethernet segment exceeds 60 per second, the corresponding event can cause a trap message to be sent to one or more management stations.

An event is generated by the RMON agent, which could be triggered by a threshold crossing. An event can be signaled as a trap, a new entry in the MIB log table, both, or neither.

inform request—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event occurred. SNMP inform requests are more reliable than traps because an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

Management Information Base—See MIB.

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 by SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MPLS—Multiprotocol label switching. MPLS is a method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels.

Multiprotocol Label switching—See MPLS.

Simple Network Management Protocol—See SNMP.

SNMP—Simple Network Management Protocol. Management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

threshold—The range in which you expect your network to perform. If a performance exceeds or goes below the expected bounds, you can examine these areas for potential problems. You can create thresholds for a specific device.

trap—Message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event occurred. Traps are less reliable than inform requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

VSI—Virtual Switch Interface. A proposed common control interface to Cisco switches. The VSI can manage connections and discover configuration information about the switch.

VSI controller—A controller, such as a PNNI SVC controller, Portable AutoRoute or MPLS controller, that controls a switch using the VSI.

VSI master—A V process implementing the master side of the VSI protocol in a VSI controller. Sometimes the whole VSI controller might be referred to as a "VSI Master," but this is not strictly correct. Also, the VSI master is a device that controls a VSI switch, for example, a VSI Label Switch Controller.

VSI slave—A VSI slave is either of the following:

1. A switch (when one router controls one slave) or a port card (when one router controls more than one slave) that implements the VSI.
2. A process implementing the slave side of the VSI protocol.

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:

- LANE on ATM
- LANE Implementation Considerations
- LANE Configuration Task List
- LANE Configuration Examples

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 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 serve*r on the interface is the third of the pool of MAC addresses.
- The ESI field value assigned to the *configuration server* is the fourth of the pool of MAC addresses.
- The selector field value is set to the subinterface number of the LANE component—except for the LECS, which has a selector field value of 0.

  Because the LANE components are defined on different subinterfaces of an ATM interface, the value of the selector field in an ATM address is different for each component. The result is a unique ATM address for each LANE component, even within the same router. For more information about assigning components to subinterfaces, see the "Rules for Assigning Components to Interfaces and Subinterfaces" 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 12 indicates how the values of unspecified digits are determined when an ATM address template is used:

Table 12 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.

Command	Purpose
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.
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
```

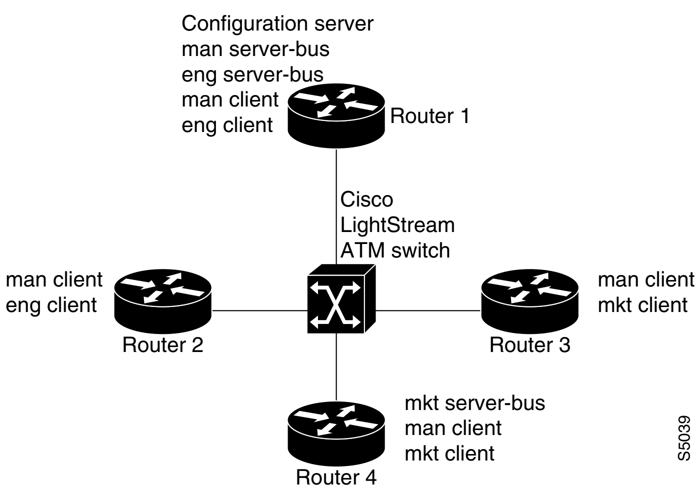
Router 4 Configuration

```
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 17. This example does not restrict membership in the emulated LANs.

Figure 17 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 13 (the ESI part of the ATM address is derived from the first MAC address of the AIP shown in the example).

Table 13 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
```

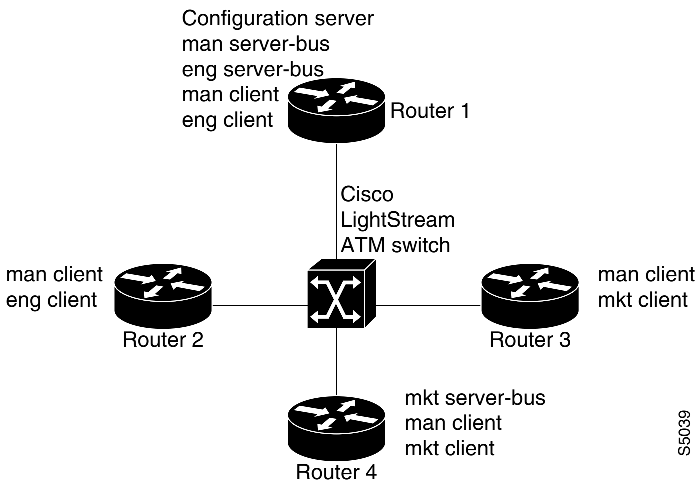
Multiple Token Ring ELANs with Restricted Membership Example

The following example, shown in Figure 18, 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 18 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

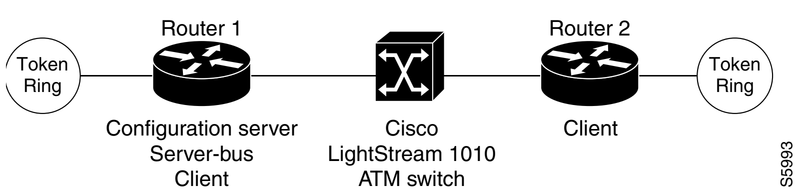
Router 4 has the server and BUS for the Marketing ELAN, a client for Marketing, and a client for Manufacturing. The first client is listed in the database as linked to the *mkt* emulated LANs. The second client is not listed in the database, but is linked to the *man* ELAN name by default. Router 4 is 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 19. This example does not restrict membership in the emulated LANs.

Figure 19 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:

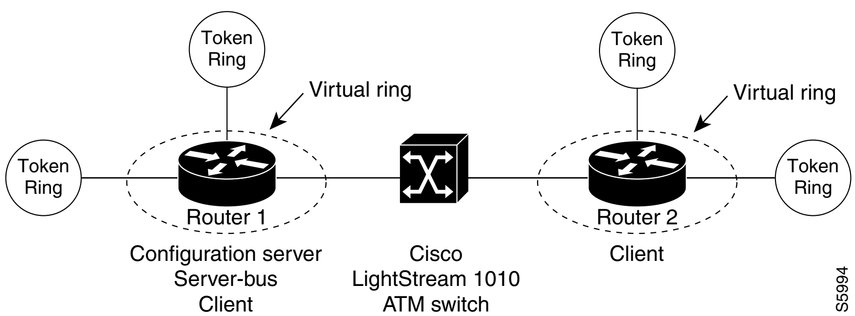
```
hostname Router2
!
interface Ethernet0/0
 ip address 10.6.10.5 255.255.255.0
!
! The following lines configure source-route bridging on the Token Ring interface.
interface TokenRing1/0
 no ip address
 ring-speed 16
 source-bridge 2 2 2048
 source-bridge spanning
!
! The following lines set up the 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 20. 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 20 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:

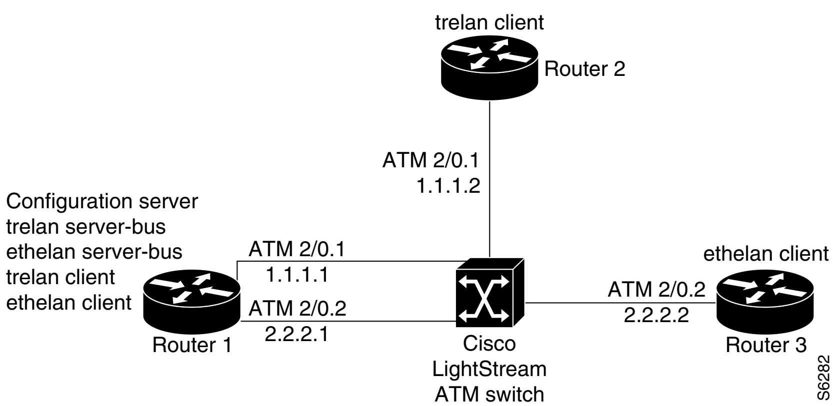
```
hostname Router2
!
! The following line configures virtual ring 512 on the router.
source-bridge ring-group 512
!
interface Ethernet0/0
 ip address 10.6.10.5 255.255.255.0
!
! The following lines configure the Token Ring interfaces.
interface TokenRing1/0
 no ip address
 ring-speed 16
 source-bridge 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 21, 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 21 Routing Between Token Ring and Ethernet Emulated LANs



Router 1 Configuration

Router 1 contains the LECS, a LES and BUS for each ELAN, and a client for each ELAN. Router 1 is configured as shown in this example:

```
hostname router1
!
! The following lines name and configures the configuration server's database.
! The server addresses for trelan and ethelan and the ELAN ring number for
! trelan are entered into the database. The default ELAN is trelan.
lane database cisco_eng
 name trelan server-atm-address 39.020304050607080910111213.00000CA05B41.01
 name trelan local-seg-id 2048
 name ethelan server-atm-address 39.020304050607080910111213.00000CA05B41.02
 default-name trelan
!
! The following lines enable the configuration server and associate it
! with the cisco_eng database.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database cisco_eng
!
```

```
! The following lines configure the tokenring LES/BUS and LEC for trelan
! on subinterface atm2/0.1 and assign an IP address to the subinterface.
interface ATM2/0.1 multipoint
 ip address 10.1.1.1 255.255.255.0
 lane server-bus tokenring trelan
 lane client tokenring trelan
!
! The following lines configure the Ethernet LES/BUS and LEC for ethelan
! on subinterface atm2/0.2 and assign an IP address to the subinterface.
interface ATM2/0.2 multipoint
 ip address 20.2.2.1 255.255.255.0
 lane server-bus ethernet ethelan
 lane client ethernet ethelan
!
! The following lines configure the IGRP routing protocol to enable routing
! between ELANS.
router igrp 1
 network 10.0.0.0
 network 20.0.0.0
```

Router 2 Configuration

Router 2 contains a client for *trelan* (Token Ring). Router 2 is configured as follows:

```
hostname router2
!
! The following lines set up the signalling and ILMI PVCs for the interface.
interface ATM2/0
 no ip address
 no keepalive
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
!
! The following lines configure a Token Ring LEC on atm2/0.1 and assign
! an IP address to the subinterface.
interface ATM2/0.1 multipoint
 ip address 10.1.1.2 255.255.255.0
 lane client tokenring trelan
!
! The following lines configure the IGRP routing protocol to enable routing
! between ELANS.
router igrp 1
 network 10.0.0.0
 network 20.0.0.0
```

Router 3 Configuration

Router 3 contains a client for *ethelan* (Ethernet). Router 3 is configured as follows:

```
hostname router3
!
! The following lines set up the signalling and ILMI PVCs for the interface.
interface ATM2/0
 no ip address
 no ip mroute-cache
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
!
! The following lines configure an Ethernet LEC on atm2/0.1 and assign
! an IP address to the subinterface.
interface ATM2/0.1 multipoint
 ip address 20.2.2.2 255.255.255.0
```

```
 lane client ethernet ethelan
!
! The following lines configure the IGRP routing protocol to enable routing
! between ELANS.
router igrp 1
 network 10.0.0.0
 network 20.0.0.0
```

Disabling LANE Flush Process Example

The following example shows a running configuration and the LE_FLUSH process disabled for all LECs:

```
more system:running-config
Building configuration...

Current configuration :496 bytes
!
! Last configuration change at 11:36:21 UTC Thu Dec 20 2001
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname donner_b
!
no lane client flush
!
interface ATM0
 atm preferred phy A
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 no atm ilmi-keepalive
!
interface ATM0.1 multipoint
 lane config-atm-address 47.00918100000001007385101.0050A2FEBC43.00
 lane client ethernet 100 elan1
!
line con 0
line vty 0 4
 no login
!
end
```

Configuring Token Ring LAN Emulation

This chapter describes how to configure Token Ring LAN emulation (LANE) on the Catalyst 5000 platform. This feature is supported on the following Catalyst 5000 series ATM modules:

- ATM Dual PHY OC-12 modules (WS-X5161 and WS-X5162)
- ATM Dual OC-3 modules (WS-5167 and WS-X5168)

Support for the Token Ring LANE feature was first introduced in Cisco IOS Release 12.0(7)T.

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

This chapter contains the following sections:

- Token Ring LANE on ATM
- Network Support
- Restrictions
- Prerequisites
- Token Ring LANE Configuration Task List
- Token Ring LANE Configuration Example

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."

Token Ring LANE on ATM

LANE bridges LAN traffic across an ATM network. The Catalyst 5000 Series Token Ring LANE feature emulates an IEEE 802.5 Token Ring LAN using ATM technology. LANE is transparent to upperlayer protocols and applications. No changes are required to existing upperlayer protocols and applications. With Token Ring LANE, Token Ring packets are encapsulated in the appropriate ATM cells and sent across the ATM network. When the packets reach the other side of the ATM network, they are deencapsulated.

Benefits

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (constant transmission delay and guaranteed capacity) with those of packet switching (flexibility and efficiency for intermittent traffic). Like X.25 and Frame Relay, ATM defines the interface between the user equipment (such as workstations and routers) and the network (referred to as the User-Network Interface [UNI]).

Token Ring LANE allows Token Ring LAN users to take advantage of the benefits of ATM without modifying end-station hardware or software. ATM uses connection-oriented service with point-to-point signalling or multicast signalling between source and destination devices. However, Token Ring LANs use connectionless service. Messages are broadcast to all devices on the network. With Token Ring LANE, routers and switches emulate the connectionless service of a Token Ring LAN for the end stations.

By using Token Ring LANE, you can scale your networks to larger sizes while preserving your investment in LAN technology.

Note The Catalyst 5000 series Cisco IOS Token Ring LANE software does not support Ethernet LANE or RFC 1483 permanent virtual connections (PVCs).

LANE Token Ring Components

LANE defines emulated LANs (ELANs). An ELAN consists of the following components:

- LANE client (LEC)—A LEC emulates a LAN interface to higher-layer protocols and applications. It forwards data to other LANE components and performs LANE address resolution functions. Each LEC is a member of only one ELAN. However, a switch or a Catalyst ATM module can include LECs for multiple ELANs; there is one LEC for each ELAN of which it is a member.

  If a switch has LECs for multiple ELANs, the switch can route traffic between ELANs.
- LANE server (LES)—The LES is the control center for an ELAN. It provides joining, address resolution, and address registration services to the LECs in that ELAN. LECs can register destination unicast and multicast MAC address with the LES. The LES also handles LANE Address Resolution Protocol (LE_ARP) requests and responses and maintains a list of route descriptors that is used to support source-route bridging (SRB) over ELANs. The route descriptors are used to determine the ATM address of the next hop in the frame's routing information field (RIF).

  There is one LES per ELAN.
- LANE broadcast and unknown server (BUS)—The BUS floods unknown destination traffic and forwards multicast and broadcast traffic to LECs within an ELAN.

  One combined LES and BUS is required for each ELAN.
- LANE Configuration Server (LECS)—The LECS contains the database that determines which ELAN a device belongs to (each LECS can have a different database). Each LEC contacts the LECS once to determine which ELAN it should join. The LECS returns the ATM address of the LES for that ELAN.

  One LECS is required for each ATM LANE switch cloud.

  The LECS database can have the following four types of entries:
  - ELAN name, ATM address of LES pairs
  - ELAN name and the ring number of the ELAN (local-seg-id)

  - LEC MAC address, ELAN name pairs
  - LEC ATM template, ELAN name pairs
  - Default ELAN name

Note An ELAN name must be unique on an interface. If two interfaces participate in LANE, the second interface may be in a different switch cloud.

The server assigns individual LECs to particular ELANs by directing them to the LES for the ELAN. The LECS maintains a database of LEC and server ATM or MAC addresses and their ELANs. A LECS can serve multiple ELANs.

- Fast Simple Server Redundancy Protocol (FSSRP)—Token Ring LANE relies on three servers: LECS, LES, and BUS. If any one of these servers fails, the ELAN cannot fully function.

  Cisco has developed a fault tolerant mechanism known as Simple Server Redundancy Protocol (SSRP) that eliminates these single points of failure. Although there is only one LES per ELAN, SSRP allows you to configure redundant servers. You can configure servers to act as backup servers that become active if a master server fails. The priority levels for the servers determine which servers have precedence.

  FSSRP is an enhancement to the SSRP. With FSSRP, LECs no longer need to go down whenever there is a change in the master LES. This uninterrupted service is achieved by connecting the LECs simultaneously to more than one LES/BUS (up to four) so that if the master LES goes down, the backup LESs are immediately available. With the basic SSRP, the LEC must go down and completely recycle before coming back up. This operation is accomplished by keeping the control connections open to all of the active LESs and BUSs in the ELAN. Although this method uses more virtual circuits (VCs), the main benefits are the transparency and speed in the switchover.

Note ELAN components coexist on one or more Cisco routers or Catalyst switches that contain an ATM module. On Cisco routers or Catalyst switches the LES and the BUS are combined into a single entity.

Network Support

The Token Ring LANE on the Catalyst 5000 series ATM module feature supports the following networking features:

- LAN switching between ELANs and between a Token Ring ELAN and a legacy LAN
- Two-port and multiport SRB between ELANs and between ELANs and a Token Ring LAN
- SRB, source-route transparent bridging (SRT), and source-route switching

The Cisco implementation of LANE over IEEE 802.5 uses existing terminology and configuration options for Token Rings and provides for the IEEE 802.5 transport of Token Ring frames across an ATM switching fabric.

Restrictions

Before you implement Token Ring LANE, be aware of the following restrictions:

Caution While VLAN Trunking Protocol (VTP) Version 2 must be enabled on a Catalyst 5000 for Token Ring to function, do not use VTP to distribute VLAN configuration information between the switches. Configure the switches to operate in VTP transparent mode and manually configure the VLANs on each switch.

- If you plan to run both Ethernet and Token Ring LANE, the Ethernet LANE software and the Token Ring LANE software must be run on separate ATM modules.
- All ATM switches have identical lists of the global LECS addresses with the identical priorities.
- Ensure that the spanning-tree port cost and priority for the ATM port are configured so that the ATM port is the preferred path (the lowest port cost with the highest priority).
- Only one LEC can be defined for each subinterface. Up to 256 subinterfaces per ATM module can be configured.
- Do not create more than one LEC for each Token Ring Bridge Relay Function (TrBRF) in each ATM module.

  While you can have only one LEC for each TrBRF in each module, you can have more than one module installed. These additional modules allow you to have more than one LEC per TrBRF, which means the module can participate in more than one ELAN. The ELANs, however, cannot be parallel or the Spanning-Tree Protocol will block one of the connections.

  Note Configuring more than one LEC for a TrBRF on a single ATM module will adversely affect frame forwarding.

- Do not configure parallel ELANs within a TrBRF (parallel ELANs are those ELANs that form a loop between switches).
- Do not create more than one LEC for each Token Ring Concentrator Relay Function (TrCRF) per ATM module.
- Ensure that all-routes explorer (ARE) reduction is enabled (using the **set tokenring reduction enable** command) on the Token Ring module.
- The number of LESs that can be defined per ELAN is unlimited; however, only one LES per ELAN can be active at a time.
- When a LECS switchover occurs, no previously joined clients are affected.
- In a LES/BUS switchover, there is a momentary loss of clients until all clients are transferred to the new LES/BUS.
- LECSs automatically come up as masters until a higher-level LECS takes priority.
- Using FSSRP, you can configure redundant LESs or BUSs and LECSs to reduce the possibility of a server failure resulting in loss of communication on the LANE network. With redundant LES/BUSs and LECSs, LANE components can switch automatically to the backup LES/BUS or LECS if the primary server fails. For specific information on how to configure FSSRP, refer to the "Configuring Fast SSRP for Redundant LANE Services" section.

Note FSSRP works only with LECS and LES/BUS combinations on Cisco devices. Third-party LANE components interoperate with the LECS and LES/BUS functions of Cisco devices but cannot take advantage of the redundancy features. Additionally, FSSRP-unaware LECs on Cisco equipment cannot take advantage of FSSRP LES/BUS redundancy.

- When a higher-priority LES comes online, it bumps the current LES off the same ELAN. For a short time after power on, some clients might change from one LES to another, depending upon the order of the LESs coming up.
- If no LES/BUS pair is up or connected to the master LECS, and more than one LES/BUS is defined for an ELAN, the LECS rejects any configuration request for that specific ELAN.
- Changes made to the list of LECS addresses on ATM switches can take up to 1 minute to propagate through the network. Changes made to the LECS database regarding LES addresses take effect almost immediately.
- If no LECS is operational or reachable, the "well-known" LECS address defined by the ATM Forum is used.
- The LECS to be used can be overridden on any subinterface by entering the following command:

  lane config-atm address *atm-address template*

Note To avoid affecting the LES/BUS or LEC redundancy, do not override any LECS, LES, or BUS addresses.

- In an underlying ATM network failure, there can be multiple master LECS and multiple active LESs or BUSs for the same ELAN, resulting in a partitioned network. Clients continue to operate normally, but transmission between partitions of the network is not possible. The system recovers when the network break is repaired.

Prerequisites

Token Ring LANE requires that the Catalyst 5000 series switch contain one of the following ATM modules running ATM software Release 4.9b or later:

- ATM Dual PHY OC-12 (WS-X5161 and WS-X5162)
- ATM Dual PHY OC-3 (WS-X5167 and WS-X5168)

These ATM modules provide an ATM network interface for the Catalyst 5000 series switch. Network interfaces reside on modular interface processors, which provide a direct connection between the high-speed synergy backplane and the external networks. The maximum number of ATM modules that the switch supports depends on the bandwidth configured.

The Catalyst 5000 series Token Ring LANE software also requires the Catalyst 5000 series supervisor engine software Release 4.3(1a) or later and one of the following switches:

- Cisco LightStream 1010 with Cisco IOS Release 12.0(1)W5 or later (recommended)
- Any ATM switch with UNI 3.0/3.1 and Interim Local Management Interface (ILMI) support for communicating the LECS address

Note If you plan to run both Ethernet and Token Ring LANE, the Ethernet LANE software and the Token Ring LANE software must be run on separate ATM modules.

Token Ring LANE Configuration Task List

To configure Token Ring LANE, complete the tasks described in the following sections:

- Opening a Session from the Switch to the ATM Module
- Creating a LANE Plan and Worksheet
- Configuring the ATM Module from the Terminal
- Configuring the ATM Module from NVRAM
- Configuring the Prefix on the LightStream 1010 Switch
- Setting Up the Signalling PVC
- Displaying LANE Default Addresses
- Entering the LECS ATM Address on the LightStream 1010 Switch
- Configuring the LECS Database
- Binding the LECS to the ATM Interface
- Setting Up a LES/BUS and a LEC
- Configuring Redundant LANE Services
- Verifying the LANE Setup
- Monitoring and Maintaining LANE Components

Note There can be multiple LECSs in an ATM cloud.

Before configuring Token Ring LANE, you must first open a session with the ATM module in the Catalyst 5000 series switch by entering the **session** line configuration command from the supervisor Console> prompt. After opening the session, you see the ATM> prompt. You only have direct access to the ATM module with which you have established a session.

Note The ATM module uses a subset of the Cisco IOS software. Generally, the Cisco IOS software works the same on the ATM module as it does on routers. After configuring the ATM module, you are ready to implement LANE.

Opening a Session from the Switch to the ATM Module

Use the **session** *mod_num* line configuration command to open a session to the ATM module from the Catalyst 5000 family switch in which the module is installed.

This example shows how to create a session to an ATM module installed in slot 5 of the Catalyst 5000 switch:

```
Console> (enable) session 5
Trying ATM-5...
```

```
Connected to ATM-5.
Escape character is '^]'.

ATM>
```

After opening the session, you see the ATM> prompt. You then have direct access only to the ATM module with which you have established a session.

Note The ATM module uses a subset of Cisco IOS software. Generally, Cisco IOS software works the same on the ATM module as it does on routers.

To configure the ATM module, you must use the ATM configuration mode in the Cisco IOS software. To enter global configuration mode, enter the **configure** EXEC command at the privileged EXEC prompt (ATM#). You see the following message, which asks you to specify the terminal, the NVRAM, or a file stored on a network server as the source of configuration commands:

```
Configuring from terminal, memory, or network [terminal]?
```

If you specify terminal, the run-time configuration is used. You can then save the run-time configuration into the NVRAM. If you specify memory, the run-time configuration is updated from the NVRAM. If you specify network, the run-time configuration is updated from a file in a server on the network.

Note You cannot configure from the network.

The ATM module accepts one configuration command per line. You can enter as many configuration commands as you want.

You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!) or pound sign (#). Comments are *not* stored in NVRAM or in the active copy of the configuration file. In other words, comments do not appear when you list the active configuration with the **write terminal** EXEC command or list the configuration in NVRAM with the **show configuration** EXEC command. Comments are stripped out of the configuration file when it is loaded to the ATM module.

Creating a LANE Plan and Worksheet

Before you begin to configure Token Ring LANE, you must decide whether you want to set up one or multiple ELANs. If you set up multiple ELANs, you must also decide where the servers and LECs will be located, and whether to restrict the clients that can belong to each ELAN. Bridged ELANs are configured just like any other LAN, in terms of commands and outputs. Once you have made those decisions, you can configure Token Ring LANE.

Before implementing Token Ring LANE, it might help you to begin by drawing up a plan and a worksheet for your own LANE scenario, showing the following information and leaving space to note the ATM address of each LANE component on each subinterface for each participating switch:

- Catalyst 5000 series switch interface where the LECS will be located.
- Catalyst 5000 series switch interface and subinterface where the LES/BUS for each ELAN will be located. For fault-tolerant operation, multiple servers can be on each ELAN.
- Catalyst 5000 series switch ATM modules, subinterfaces, and VLANs where the LECs for each ELAN will be located.

- Name of the default ELAN (optional). The default Token Ring ELAN is the same as the default TrCRF (1003). You can use the default Token Ring ELAN (trcrf-default) or configure a new one.
- Names of the ELANs that will have unrestricted membership.
- Names of the ELANs that will have restricted membership.
- Local segment ID for the ELAN. The local segment ID must be identical to the ring number of the TrCRF.

Note The last three items in the list above are important because they determine how you set up each ELAN in the LECS database.

Default LANE Configuration

Table 14 shows the default LANE configuration.

Table 14 Default LANE Configuration

Feature	Default Value
LANE components	No LECS database is configured. No LES/BUS is configured. No LECs are configured.
PVCs	ILMI and signalling PVCs are set up.
Preferred PHY (Dual PHY modules only)	PHY A
Output throttling	Disabled
ILMI keepalives	Disabled
UNI version	Autonegotiate (reverts to UNI 3.0 if autonegotiation fails)
VTP	Disabled

Configuring the ATM Module from the Terminal

To configure the ATM module from the terminal, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`ATM#` **`configure terminal`**	Selects the terminal option and enters global configuration mode.
Step 2	`ATM(config)#` **`interface atm`** *`elanname`*	Selects an ATM ELAN subinterface.
Step 3	`ATM(config-if)#` **`lane client tokenring`** *`elanname`*	Identifies the ELAN attached to this subinterface as a Token Ring ELAN.
Step 4	`ATM(config-if)#` **`Ctrl-Z`**	Exits global configuration mode.
Step 5	`ATM(config)#` **`write memory`**	Saves the configuration file modifications to NVRAM.

In the following example, the ATM module is configured from the terminal. The **interface atm 0** interface configuration command designates that ATM interface 0 is to be configured. The **lane client tokenring** command links TrCRF 10 to the ELAN named trcrf-10. The **Ctrl-Z** command quits configuration mode. The **write memory** command loads the configuration changes into NVRAM on the ATM module.

```
ATM# configure terminal
ATM (config)# interface atm 0
ATM (config-subif)# lane client tokenring 10 trcrf-10
ATM (config-subif)# Ctrl-Z
ATM# write memory
```

NVRAM stores the current configuration information in text format as configuration commands, recording only nondefault settings. The ATM module software performs a memory checksum to guard against corrupted data.

As part of its startup sequence, the ATM module startup software always checks for configuration information in NVRAM. If NVRAM holds valid configuration commands, the ATM module executes the commands automatically at startup. If the ATM module detects a problem with its NVRAM or the configuration it contains, the module goes into default configuration. Problems can include a bad checksum for the information in NVRAM or the absence of critical configuration information.

Configuring the ATM Module from NVRAM

To configure the ATM module from NVRAM, reexecute the configuration commands in privileged EXEC mode:

Command	Purpose
ATM(config)# **configure memory**	Configures the ATM module from NVRAM.

Configuring the Prefix on the LightStream 1010 Switch

Before you configure LANE components on a Catalyst 5000 series switch ATM module, you must configure the Cisco LightStream 1010 switch with the ATM address prefix to be used by all LANE components in the switch cloud.

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

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

Note On the Cisco LightStream 1010 switch, the ATM address prefix is called the *node ID.* Prefixes must be 26 digits long. If you provide fewer than 26 digits, zeros are added to the right of the specified value to fill it to 26 digits. LANE prefixes must start with 39 or 47.

Note If you do not save the configured value permanently, it will be lost when the switch is reset or powered off.

To display the current prefix on the Cisco LightStream 1010 switch, use the **show network** EXEC command.

Setting Up the Signalling PVC

You must set up the signalling PVC and the PVC that will communicate with the ILMI on the major ATM interface of any Catalyst 5000 series switch that participates in LANE. Complete this task only once for a major interface. You need not repeat this task on the same interface even though you might configure LESs and clients on several of its subinterfaces.

To set up these PVCs, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`ATM(config)#` **`interface atm`** *`slot/port`*	Specifies the major ATM interface and enters interface configuration mode.
Step 2	`ATM(config)#` **`atm pvc`** *`vcd vpi vci`* **`qsaal`**	Establishes the signalling PVC that sets up and tears down switched virtual circuits (SVCs); the *vpi* and *vci* values are usually set to 0 and 5, respectively. The *vcd* is the virtual channel descriptor.
Step 3	`ATM(config)#` **`atm pvc`** *`vcd vpi vci`* **`ilmi`**	Sets up a PVC to communicate with the ILMI; the *vpi* and *vci* values are usually set to 0 and 16, respectively.

Displaying LANE Default Addresses

You can display the LANE default addresses to make configuration easier. Complete this task for each Catalyst 5000 series switch ATM interface that participates in LANE. The **show lane default-atm-address** EXEC command displays default addresses for all ATM interfaces present on the switch. Write down the displayed addresses on your LANE worksheet.

To display the default LANE addresses, use the following command in global configuration mode:

Command	Purpose
`ATM#` **`show lane default-atm-addresses`** `[`**`interface atm`** *`number`*`[.`*`subinterface-number`*`]]`	Displays the LANE default addresses.

Entering the LECS ATM Address on the LightStream 1010 Switch

You must enter the LECS ATM address into each ATM switch (such as a Cisco LightStream 1010 ATM switch) connected to an ATM module in your LANE network and save the address permanently so that the value will not be lost when the switch is reset or powered off. Programming the LECS addresses allows the LESs and LECs to determine the LECS addresses dynamically through ILMI.

To enter a LECS ATM address into a LightStream 1010 switch and save it there permanently, use the following commands on the Cisco LightStream 1010 switch beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)#` **`atm lecs-address-default`** ***`address1`*** `[`*`address2...`*`]`	Specifies the LECS's ATM address for the entire switch. Use the addresses from your LANE worksheet and specify the full 40-digit ATM address.
Step 2	`Router(config)#` **`exit`**	Exits global configuration mode.
Step 3	`Switch#` **`copy running-config startup-config`**	Saves the configuration value permanently.

Configuring the LECS Database

The LECS database contains LANE configuration information, including ELAN name-to-LES/BUS ATM address mappings, LEC address-to-ELAN name mappings, and the name of the default ELAN, if specified. You must configure at least one LECS database in the LANE network.

When configuring the LECS database, remember the following guidelines:

- You can configure redundant LECSs. Redundant LECSs should be configured on different devices in the LANE network. If you configure more than one LECS, make sure that all databases with the same name are identical.
- You can specify one default ELAN in the database. The LECS assigns any client that does not request a specific ELAN to the default ELAN.
- ELANs are either restricted or unrestricted. The LECS assigns a client to an unrestricted ELAN if the client specifies that particular ELAN in its configuration. However, the LECS only assigns a client to a restricted ELAN if the client is specified in the LECS's database as belonging to that ELAN. The default ELAN should have unrestricted membership.
- If you are configuring fault tolerance, you can have any number of servers per ELAN. Priority is determined by entry order; the first entry has the highest priority unless you override it with the index option.

When setting up the LECS database remember that the following are requirements when configuring LECs:

- The VLAN name must match the ELAN name.
- The ring number defined when configuring the VLAN must match the local segment ID.

  The **set vlan** interface configuration command assumes that any ring number you enter is in hexadecimal. Therefore, 12 is stored as the hexadecimal value 0x12. The **name** *elan_name* **local-seg-id** *segment_number* LANE database configuration command assumes that any value you enter for the **local-seg-id** is in decimal unless you enter it explicitly in hexadecimal. For example, to define a TrCRF with a ring number of 12 you could enter the **set vlan 12 name crf12 type trcrf ring 12 parent 100** interface configuration command or the **set vlan 12 name crf12 type trcrf ring 0x12 parent 100** interface configuration command.

  When defining a corresponding LEC, you could enter the **name crf12 local-seg-id 0x12** or **name crf12 local-seg-id 18** LANE database configuration command because 18 is the decimal equivalent of 0x12.

To set up the database, complete the tasks in the following sections as appropriate for your ELAN plan and scenario:

- Setting Up the Database for the Default ELAN
- Setting Up the Database for Unrestricted-Membership ELANs
- Setting Up the Database for Restricted-Membership ELANs

Setting Up the Database for the Default ELAN

When you configure a Catalyst 5000 series switch ATM module as the LECS for one default ELAN, you need to provide the following information:

- A name for the database
- The ATM address of the LES for the ELAN
- A default name for the ELAN

In addition, you indicate that the LECS's ATM address is to be computed automatically.

The default ELAN cannot be a restricted-membership ELAN. You do not need to specify the ATM or MAC addresses of the LECs for the default ELAN.

On the Dual PHY ATM modules, you must configure redundant LESs or BUSs and a LECS, one for each PHY.

When you configure a database with only a default unrestricted ELAN, you need not specify where the LECs are located. That is, when you set up the LECS's database for a single default ELAN, you need not provide any database entries that link the ATM addresses of any clients with the ELAN name. All of the clients are automatically assigned to a default ELAN.

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

	Command	Purpose
Step 1	`ATM(config)#` **lane database** *database-name*	Enters database configuration mode for the LANE database that you specify.
Step 2	`ATM(lane-config-database)#` **name** *elan-name* **server-atm-address** *atm-address* [**index** *n*]	Binds the name of the ELAN to the ATM address of the LES in the configuration database. The index determines the priority. The highest priority is 0. Enter the ATM address of the server for the specified ELAN, as noted in your LANE worksheet and obtained in the "Displaying LANE Default Addresses" section. You can have any number of servers per ELAN for fault tolerance. Priority is determined by entry order. The first entry has the highest priority unless you override it with the index number.

	Command	Purpose
Step 3	`ATM(lane-config-database)#` **`name`** *`elan-name`* **`local-seg-id`** *`segment-number`*	Assigns a segment number to the emulated Token Ring LAN in the configuration database. The segment number you specify for the **local-seg-id** keyword must remain the same for each entry you add and it must also be identical to the ring number of the TrCRF. The **set vlan** interface configuration command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal.
Step 4	`ATM(lane-config-database)#` **`default-name`** *`elan-name`*	Provides a default name for the ELAN in the configuration database. If you are setting up only a default ELAN, the *elan-name* argument in Step 2 and Step 3 is the same as the default ELAN name you provide in Step 4.
Step 5	`ATM(lane-config-database)#` **`exit`**	Exits from database configuration mode and returns to global configuration mode.

Note After you configure the LECS database, you must bind the LECS database to the major ATM interface (ATM0) on the ATM module. For information on how to bind the database to the interface, see the "Binding the LECS to the ATM Interface" section later on in this chapter.

Setting Up the Database for Unrestricted-Membership ELANs

When you configure unrestricted-membership ELANs in the LECS database, you create database entries that link the name of each ELAN to the ATM address of its LES/BUS.

However, you may choose *not* to specify where the LECs are located. That is, when you set up the LECS's database, you do not have to provide any database entries that link the ATM addresses or MAC addresses of any clients with the ELAN name. The LECS assigns the clients to the ELANs specified in the client's configurations.

Note In the steps listed in the task table, enter the ATM address of the server for the specified ELAN, as noted in your LANE worksheet and obtained in the Displaying LANE Default Addresses section earlier in this chapter.

To configure unrestricted-membership ELANs in the LECS database, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`ATM(config)# lane database database-name`	Enters database configuration mode for the LANE database that you specify.
Step 2	`ATM(lane-config-database)# name elan-name1 server-atm-address atm-address [index n]`	Binds the name of the first ELAN to the ATM address of the LES/BUS for that ELAN in the configuration database. The index determines the priority. The highest priority is 0.
Step 3	`ATM(lane-config-database)# name elan-name2 server-atm-address atm-address [index n]`	Binds the name of the second ELAN to the ATM address of the LES/BUS in the configuration database. The index determines the priority. The highest priority is 0. Repeat this step, providing a different ELAN name and ATM address for each additional ELAN in this switch cloud.
Step 4	`ATM(lane-config-database)# name elan-name1 local-seg-id segment-number`	Assigns a segment number to the first emulated Token Ring LAN in the configuration database. The segment number you specify for **local-seg-id** must be identical to the ring number of the TrCRF. The **set vlan** command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* command assumes that any value you enter for the **local-seg-id** is in decimal unless you enter it explicitly in hexadecimal.
Step 5	`ATM(lane-config-database)# name elan-name2 local-seg-id segment-number`	Assigns a segment number to the second emulated Token Ring LAN in the configuration database. The segment number you specify for **local-seg-id** must be identical to the ring number of the TrCRF. The **set vlan** command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* command assumes that any value you enter for the **local-seg-id** is in decimal unless you enter it explicitly in hexadecimal. Repeat this step, providing a different ELAN name and segment number for each additional source-route bridged ELAN in this switch cloud.
Step 6	`ATM(lane-config-database)# default-name elan-name`	(Optional) Specifies a default ELAN for LECs not explicitly bound to an ELAN.
Step 7	`ATM(lane-config-database)# exit`	Exits database configuration mode and returns to global configuration mode.

Setting Up the Database for Restricted-Membership ELANs

When you configure restricted-membership ELANs in the LECS database, you create database entries that link the name of each ELAN to the ATM address of its LES/BUS.

Unlike unrestricted-membership, you must *also* specify where the LECs are located. That is, for each restricted-membership ELAN, you provide a database entry that explicitly links the ATM address or MAC address of each client of that ELAN with the name of that ELAN.

Those client database entries specify which clients are allowed to join the ELAN. When a client requests to join an ELAN, the LECS consults its database and then assigns the client to the ELAN specified in the LECS's database.

When clients for the same restricted-membership ELAN are located in multiple switch ATM interfaces, each client's ATM address or MAC address must be linked explicitly with the name of the ELAN. As a result, you must configure as many client entries as you have clients for ELANs in all the switch ATM interfaces. Each client will have a different ATM address in the database entries.

To configure restricted-membership ELANs in the LECS database, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`ATM(config)#` **`lane database`** *`database-name`*	Enters database configuration mode for the LANE database that you specify.
Step 2	`ATM(lane-config-database)#` **`name`** *`elan-name1`* **`server-atm-address`** *`atm-address`* **`restricted`** `[`**`index`** *`n`*`]`	Binds the name of the first ELAN to the ATM address of the LES/BUS for that ELAN in the configuration database. If you are configuring SSRP, repeat this step with the same ELAN name but with different server ATM addresses for each additional server for the same ELAN. The index determines the priority. The highest priority is 0.
Step 3	`ATM(lane-config-database)#` **`name`** *`elan-name2`* **`server-atm-address`** *`atm-address`* **`restricted`** `[`**`index`** *`n`*`]`	Binds the name of the second ELAN to the ATM address of the LES/BUS in the configuration database. The index determines the priority. The highest priority is 0. Repeat this step, providing a different name and a different ATM address, for each additional ELAN.
Step 4	`ATM(lane-config-database)#` **`name`** *`elan-name1`* **`local-seg-id`** *`segment-number`*	Assigns a segment number to the first emulated Token Ring LAN in the configuration database. The segment number you specify for the **local-seg-id** keyword must be identical to the ring number of the TrCRF. The **set vlan** interface configuration command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal.

	Command	Purpose
Step 5	`ATM(lane-config-database)#` **`name`** *`elan-name2`* **`local-seg-id`** *`segment-number`*	Assigns a segment number to the second emulated Token Ring LAN in the configuration database. The segment number you specify for the **local-seg-id** keyword must be identical to the ring number of the TrCRF. The **set vlan** interface configuration command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal. Repeat this step, providing a different ELAN name and segment number for each additional source-route bridged ELAN in this switch cloud.
Step 6	`ATM(lane-config-database)#` **`client-atm-address`** *`atm-address-template`* **`name`** *`elan-name`*	Adds a database entry associating a specific client's ATM address with a specific restricted-membership ELAN. Repeat this step for each of the clients of each of the restricted-membership ELANs on the switch cloud, in each case specifying that client's ATM address and the name of the ELAN with which it is linked.
Step 7	`ATM(lane-config-database)#` **`exit`**	Exits from database configuration mode and returns to global configuration mode.

Binding the LECS to the ATM Interface

Once you have created the database entries as appropriate to the type and the membership conditions of the ELANs, to enable the LECS on the selected ATM interface and switch, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`ATM(config)#` **`interface atm`** *`number`*	If you are not currently configuring the interface, specifies the major ATM interface where the LECS is located and enters interface configuration mode.
Step 2	`ATM(config-if)#` **`lane config auto-config-atm-address`**	Specifies that the LECS's ATM address will be computed by the automatic method.
Step 3	`ATM(config-if)#` **`lane config database`** *`database-name`*	Binds the LECS's database name to the specified major interface, and enables the LECS.
Step 4	`ATM(config-if)#` **`exit`**	Exits interface configuration mode.
Step 5	`ATM#` **`copy running-config startup-config`**	Saves the configuration.

Setting Up a LES/BUS and a LEC

For each Catalyst 5000 series switch ATM module that will participate in LANE, set up the necessary servers and clients for each ELAN and then display and record the server and client ATM addresses. Be sure to keep track of the switch ATM interface where the LECS will eventually be located.

If you will have only one default ELAN, you only need to set up one server. If you will have multiple ELANs, you can set up the server for another ELAN on a different subinterface on the same interface of this switch, or you can place it on a different switch.

When you set up a server and BUS on a switch, you can combine them with a client on the same subinterface, a client on a different subinterface, or no client at all on the switch.

Depending on where your clients and servers are located, perform one of the following tasks for each LANE subinterface:

- Setting Up the LES/BUS for an ELAN
- Setting Up a LEC for an ELAN

Setting Up the LES/BUS for an ELAN

To set up the LES/BUS for an ELAN, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`ATM(config)#` **`interface atm`** *`number`*`[.`*`subinterface-number`*`]`	Specifies the subinterface for the first ELAN on this switch and enters interface configuration mode.
Step 2	`ATM(config-if)#` **`lane server-bus tokenring`** *`elan-name1`*	Enables a LES/BUS for the first ELAN on the subinterface (you cannot configure more than one LES/BUS per subinterface).
Step 3	Repeat Steps 1 and 2 for all LES/BUSs you want to configure on the ATM module.	
Step 4	`ATM(config-if)#` **`exit`**	Exits interface configuration mode.
Step 5	`ATM#` **`copy running-config startup-config`**	Saves the configuration.

If the ELAN specified in Step 2 is intended to have *restricted membership* in the LECS database, carefully consider whether or not you want to specify its name here. You will specify the name in the LECS database when it is set up. However, if you link the client to an ELAN in this step, and through some mistake it does not match the database entry linking the client to an ELAN, this client will not be allowed to join this ELAN or any other.

If you do decide to include the name of the ELAN linked to the client in Step 2 and later want to associate that client with a different ELAN, make the change in the LECS's database before you make the change for the client on this subinterface.

Setting Up a LEC for an ELAN

This section describes the following tasks for setting up a LEC:

- Guidelines for Setting Up a LEC
- Creating a Token Ring VLAN
- Setting Up the Token Ring VLAN on a LEC

Guidelines for Setting Up a LEC

The Catalyst 5000 series Token Ring LANE requires the following software:

- Catalyst 5000 series supervisor engine software Release 4.3(1a) and later
- ATM software Release 4.9(b) and later
- VTP Version 2

Note While VTP version 2 must be enabled on a Catalyst 5000 for Token Ring to function, do not use VTP to distribute VLAN configuration information between the switches. Configure the switches to operate in VTP transparent mode and manually configure the VLANs on each switch.

When you set up a LEC, follow these rules and recommendations:

- Make sure you properly configure the LECS and LES/BUS using the ATM module command-line interface (CLI) for each VLAN before creating a LEC. VTP does not set up the LECS or LES/BUS.
- In the **set vlan** interface configuration command, the *vlan_num* argument represents the VLAN number to configure, and the *vlan_name* argument is the name of the VLAN.
- The VLAN name must match the ELAN name and the ring number must match the local segment ID.

  The **set vlan** interface configuration command assumes that any ring number you enter is in hexadecimal. Therefore, 0x12 or 12 is stored as the hexadecimal value 0x12. The **name** *elan_name* **local-seg-id** *segment_number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal. For example, to define a TrCRF with a ring number of 12 you could enter the **set vlan 12 name crf12 type trcrf ring 12 parent 100** interface configuration command or the **set vlan 12 name crf12 type trcrf ring 0x12 parent 100** interface configuration command.

  When defining a corresponding LEC, you could enter **name crf12 local-seg-id 0x12** or **name crf12 local-seg-id 18** because 18 is the decimal equivalent of 0x12.
- Before you can create a LEC, the TrBRF and TrCRF to which it will be associated must exist.
- Do not create more than one LEC for each TrBRF per ATM module.

  While you can have only one LEC per TrBRF per module, you can have more than one module installed. This allows you to have more than one LEC per TrBRF, which means the switch can participate in more than one ELAN. The ELANs, however, cannot be parallel or the Spanning-Tree Protocol will block one of the connections.

  Note Configuring more than one LEC for a TrBRF on a single ATM module will adversely affect frame forwarding.

- Ensure that all-routes explorer (ARE) reduction is enabled (using the **set tokenring reduction enable** interface configuration command) on the Token Ring module.
- Do *not* configure parallel ELANs within a TrBRF (parallel ELANs are those ELANs that form a loop between switches).
- Do not create more than one LEC for each TrCRF per ATM module.

  A TrCRF can include only one enabled LEC from any ATM module.

An ATM module LEC is assigned to a TrCRF to provide connectivity to the ATM network. In this sense, an ATM module is a logical port within the TrCRF. When assigning enabled LECs to TrCRFs, the enabled LECs of any one ATM expansion module should each be assigned to different TrCRFs.

- You can change all ELAN names with the exception of VLANs 1, 1003, or 1005 whose ELAN names must remain **default**, trcrf-default, and trbrf-default, respectively. You cannot override the ELAN name for VLAN 1, 1003, or 1005 by using the **name** *elan_name* parameter. You can assign all other VLANs any name.

  When you enter the **set vlan** *vlan_num* [**name** *vlan_name*] interface configuration command in transparent mode and do not specify the optional **name** *elan_name* parameter, the software uses the names in Table 15 by default.

Table 15 Default VLAN ELAN Names

VLAN Number	VLAN Name
1	default
2...1002	VLAN0002 through VLAN1002
1003	trcrf-default
1004	VLAN1004
1005	trbrf-default

If you currently have a different ELAN name for VLAN 1 or VLAN 1003, you must change the ELAN name to default (for VLAN 1) or trcrf-default (for VLAN 1003) in the LECS database. The following example shows an LECS database configuration that specifies **marktng** as the ELAN name for VLAN 1003:

```
lane database test
name marktng server-atm-address 47.00918100000000061705B8301.00400B020011.01
!
interface ATM0
no ip address
no ip route-cache
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
lane config auto-config-atm-address
lane config database test
!
interface ATM0.1 multipoint
no ip route-cache
lane server-bus tokenring marktng
lane client tokenring 1003 marktng
```

You must change the ELAN name for VLAN 1003 from marktng to trcrf-default in the second and last lines of the display, as follows:

```
lane database test
name default server-atm-address 47.00918100000000061705B8301.00400B020011.01
!
interface ATM0
no ip address
no ip route-cache
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
lane config auto-config-atm-address
lane config database test
!
interface ATM0.1 multipoint
```

```
no ip route-cache
lane server-bus tokenring default
lane client tokenring 1003 trcrf-default
```

Creating a Token Ring VLAN

With Token Ring, to successfully route packets between ELANs, you can only set up one LEC for each TrBRF on an ATM module. For multiple ELANs with the same TrBRF to route packets, they must be configured on either separate ATM modules or connected via an external device.

If the TrBRF and TrCRF for which you are creating a LEC do not already exist, create the Token Ring VLANs by using the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Console> (enable) **set vlan** *vlan_num* [**name** *name*] **type trbrf** [**state** {**active** | **suspend**}] [**mtu** *mtu*] **bridge** *bridge_number* [**stp** {**ieee** | **ibm** | **auto**}]	From the supervisor module, defines the TrBRF that you will associate to TrCRF as a parent
Step 2	Console> (enable) **set vlan** *vlan_num* [**name** *name*] **type trcrf** [**state** {**active** | **suspend**}] [**mtu** *mtu*] **ring** *ring_number* **parent** *vlan_num* [**mode** {**srt** | **srb**}] [**backupcrf** {**off** | **on**}] [**aremaxhop** *hopcount*] [**stemaxhop** *hopcount*]	From the supervisor module, defines the TrCRF for which you are creating a LEC.

Setting Up the Token Ring VLAN on a LEC

To set up the LEC for the Token Ring VLAN and corresponding ELAN, use the following commands on the ATM module beginning in global configuration mode:

	Command	Purpose
Step 1	ATM(config)# **interface atm** *number*[**.***subinterface-number*]	Specifies the subinterface for an ELAN on this switch and enters interface configuration mode.
Step 2	ATM(config-if)# **lane client tokenring** ***vlan_id*** [*elan-name1*]	Creates a LEC for the first ELAN and specifies the VLAN number and the ELAN name to which to bind the LEC.
Step 3	ATM(config-if)# **exit**	Exits configuration mode.
Step 4	ATM(config)# **copy running-config startup-config**	Saves the configuration.

Configuring Redundant LANE Services

The LANE protocol does not specify where any of the ELAN server entities should be located, but for the purpose of reliability and performance, Cisco implements these server components on its routers and LAN switches.

With Phase I LANE, only one LECS, capable of serving multiple ELANs, and only one LES per ELAN could exist for an ATM cloud. The Phase I LANE protocol did not allow for multiple LESs within an ELAN. Therefore, these components represented both single points of failure and potential bottlenecks for LANE service.

LANE LES/BUS and LECS redundancy corrects these limitations by allowing you to configure redundant LES/BUSs so that the LECs in an ELAN can automatically switch to a backup LES if the primary LES fails. The priority of the LES/BUS pairs is established by the order in which they are entered in the LECS database. LANE LES/BUS and LECS redundancy is always enabled. You can use this redundancy feature by configuring multiple servers.

LES/BUS and LECS redundancy works only with Cisco LECS and LES combinations. Third-party LANE server components continue to interoperate with the LECS and LES/BUS function of Cisco routers and switches, but cannot take advantage of the redundancy features.

The following servers are single points of failure in the ATM LANE system:

- LECS (configuration server)
- LES (ELAN server)
- BUS

LES/BUS and LECS redundancy eliminates these single points of failure.

Enabling Redundant LECSs

To enable redundant LECSs, enter the multiple LECS addresses to the end ATM switches, which are used as central locations for the list of LECS addresses. After entering the LECS addresses, LANE components connected to the switches can obtain the global list of LECS addresses.

Note To configure LES/BUS and LECS redundancy, you must enable multiple, redundant, and standby LECSs and multiple, redundant, and standby LES/BUSs. The LES/BUS and LEC redundancy configuration procedure guards against failure on hardware on which LANE components are running, including all Catalyst 5000 series switches. The configuration procedure is not effective for ATM network switch failures.

To enable LES/BUS and LEC redundancy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)#` **`atm lecs-address`** *`address`*	Allows you to enter the multiple LECS addresses on the ATM switch.
Step 2	`ATM(config)#` **`name`** ***`elan-name`*** **`server-atm-address`** ***`les-address`*** `[`**`index`** *`n`*`]`	Specifies redundant LES/BUSs on the ATM module. Enter the command for each LES address on the ELAN. The index determines the priority; 0 is the highest priority.

Enabling ILMI Keepalive Timeout

If enabled, ILMI sends keepalive messages on an ongoing basis on the active physical (PHY) to the switch, and the switch responds. If the response is not obtained for the last four polls, the ILMI timer times out and the Dual PHY changes from active PHY to backup PHY. This feature is useful only if the two PHYs are connected to two different switches.

By default, this feature is disabled. To enable it, start a session to the ATM module (using the **session** command), and then enter the following commands:

```
ATM> enable
ATM# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0
ATM(config-if)# atm ilmi-keepalive 4
ATM(config-if)# end
ATM#
```

These commands enable the transmission of ILMI keepalive messages and set the time between ILMI keepalive messages to 4 seconds.

Using UNI 3.1 Signalling Support

The ATM LANE Dual PHY module supports backward compatibility with ATM switches for UNI version 3.1. On startup, ILMI negotiates between UNI versions 3.0 and 3.1, which requires no configuration. If the ILMI link autodetermination is enabled on the interface, the router or switch accepts the UNI version returned by ILMI. If the ILMI link autodetermination is unsuccessful or if ILMI is disabled, the UNI version defaults to 3.0. You can override the version number by entering the **atm uni-version** command. If ILMI is enabled when you enter the **no** version of the command, the UNI version is set to the version returned by ILMI and the link autodetermination is successful. Otherwise, the version reverts to 3.0. Enter the **no atm uni-version** command to override the UNI version.

Note Each ELAN is a separate subnetwork.

Configuring Fast SSRP for Redundant LANE Services

With FSSRP, you can configure redundant LES/BUS pairs for each ELAN. With FSSRP, which differs from the previously implemented SSRP, all configured LESs of an ELAN are active which means FSSRP-aware redundant LES/BUS pairs can accept join requests from any FSSRP-aware client.

LECs that are FSSRP aware have VCs established to every single LES/BUS in the ELAN. Because VC connections already exist between all LECs and LES/BUS pairs in the ELAN, the LECs can switch over to another LES/BUS pair without any noticeable delay should a failure occur.

When you configure more than one LES/BUS pair for an ELAN, one LES/BUS takes precedence over others based on the order in which they are entered into the LECS database.

Note Redundant LES/BUS pairs for a single ELAN should be configured on different ATM LANE modules in the LANE network for maximum fault tolerance.

Configuring redundant LES/BUS pairs for an ELAN is a two-part process:

- You must first configure the redundant LES/BUS pairs on subinterfaces for that ELAN.
- You must then enter the ATM addresses of the redundant LES/BUS pairs into the LECS database for the ELAN.

To configure the LES/BUS pairs, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`ATM# configure terminal`	Enters global configuration mode.
Step 2	`ATM (config)# interface atm0`	Specifies the major interface and enters subinterface configuration mode.

	Command	Purpose
Step 3	`ATM (config-subif)#` **`lane fssrp`**	Enables FSSRP on the major interface
Step 4	`ATM (config-subif)#` **`interface atm 0.`** *`subinterface-number`*	Specifies the subinterface for the first ELAN.
Step 5	`ATM (config-subif)#` **`lane server-bus tokenring`** *`elan-name`*	Enables the LES/BUS for an ELAN on the subinterface (you cannot configure more than one LES/BUS per subinterface).
	Repeat Steps 2 and 3 for all LES/BUSs you want to configure on this ATM module.	
Step 6	`ATM (config-subif)#` **`Ctrl-Z`**	Exits subinterface configuration mode.
Step 7	`ATM#` **`show lane server`**	Verifies the LES/BUS configuration.

Note The LES/BUSs are not fully operational until one or more LECs are configured and the LECS database is configured and bound to the ATM module interface.

This example shows how to specify the LES/BUS for an ELAN and verify the configuration:

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0.1
ATM(config-subif)# lane server-bus tokenring default
ATM(config-subif)# interface atm0.2
ATM(config-subif)# lane server-bus tokenring Eng_ELAN
ATM(config-subif)# ^Z
ATM# show lane server
LE Server ATM0.1  ELAN name: default  Admin: up  State: operational
type: tokenring        Max Frame Size: 4472
ATM address: 47.00918100000000E04FACB401.00100DAACC41.01
LECS used: 47.007900000000000000000000.00A03E000001.00 NOT yet connected

LE Server ATM0.2  ELAN name: Eng_ELAN  Admin: up  State: operational
type: tokenring        Max Frame Size: 4472
ATM address: 47.00918100000000E04FACB401.00100DAACC41.02
LECS used: 47.007900000000000000000000.00A03E000001.00 NOT yet connected
```

To add the redundant LES/BUS pairs to the LECS, use the following commands beginning in privileged EXEC configuration mode:

	Command	Purpose
Step 1	`ATM#` **`show lane server`**	Displays the ATM address of the LES/BUS for the ELAN.
Step 2	`ATM#` **`configure terminal`**	Enters global configuration mode.
Step 3	`ATM (config)#` **`lane database`** *`database-name`*	Enters database configuration mode, specifying a LANE database name.
Step 4	`ATM (lane-config-database)#` **`name`** *`elan-name`* **`server-atm-address`** *`atm-address`*	Binds the name of the ELAN to the ATM addresses of the LES/BUS pairs in the order you want the services to fail over.
Step 5	`ATM (lane-config-database)#` **`default-name`** *`elan-name`*	In the configuration database, provides a default name of the ELAN.

	Command	Purpose
Step 6	`ATM (lane-config-database)#` **`Ctrl-Z`**	Exits from database configuration mode.
Step 7	`ATM#` **`show lane database`**	Displays the LECS database configuration so that you can verify your changes.

This example shows how to display the ATM address of the LES/BUS of the default ELAN, how to configure the LECS database for the default ELAN, and how to verify the configuration:

```
ATM# show lane server
LE Server ATM0.1  ELAN name: default  Admin: up  State: operational
type: ethernet         Max Frame Size: 1516
ATM address: 47.00918100000000E04FACB401.00100DAACC41.01
LECS used: 47.007900000000000000000000.00A03E000001.00 NOT yet connected

ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# lane database LANE_Backbone
ATM(lane-config-database)# name default server-atm-address
47.00918100000000E04FACB401.00100DAACC41.01
ATM(lane-config-database)# default-name default
ATM(lane-config-database)# ^Z
ATM# show lane database

LANE Config Server database table 'LANE_Backbone'
default elan: default
elan 'default': un-restricted
  server 47.00918100000000E04FACB401.00100DAACC41.01 (prio 0)
```

Verifying the LANE Setup

Once you have set up the LECs on the subinterfaces of an ATM module, you can display their ATM addresses by using the following command in privileged EXEC mode:

Command	Purpose
`Router#` **`show lane`**	Displays the LES, BUS, and LEC ATM addresses.

The command output shows all the subinterfaces configured for LANE. For each subinterface, the command displays and labels the ATM addresses that belong to the LES, BUS, and the LEC.

When you look at each ATM address, confirm the following items:

- The prefix is the one you set up on the switch.
- The end-system identifier field reflects the base address of the pool of MAC addresses assigned to the ATM interface plus a value that represents the specific LANE component.
- The selector byte is the same number as the subinterface (converted to hexadecimal).

Enter the **show lane** EXEC command on each Catalyst 5000 series switch to verify the LANE setup before you set up the LECs on the next Catalyst 5000 series switch. Print the display or make a note of these ATM addresses so that you can use it when you set up the LECS database. At this point in the configuration process, the LECs are not normally operational.

Monitoring and Maintaining LANE Components

After configuring LANE components on an interface or any of its subinterfaces, you can display their status on a specified subinterface or on an ELAN. To show LANE information, issue the following commands in privileged EXEC mode:

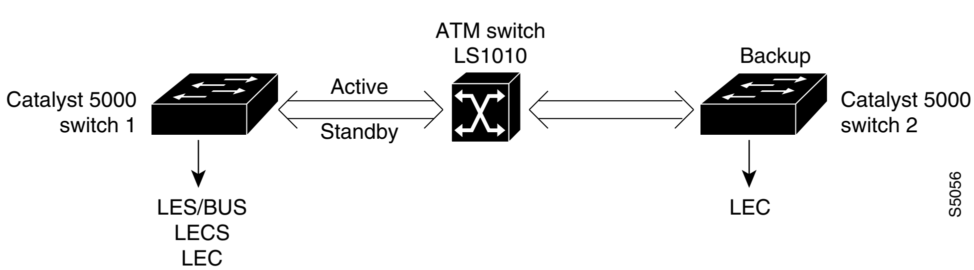
Command	Purpose
Router# **show lane** [**interface atm 0** [*subinterface-number* | **name** *elan-name*]] [**brief**]	Displays the global and per-VCC LANE information for all the LANE components and ELANs configured on an interface or any of its subinterfaces.
Router# **show lane bus** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for the BUS configured on any subinterface or ELAN.
Router# **show lane client** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for all LECs configured on any subinterface or ELAN.
Router# **show lane config** [**interface atm 0**]	Displays the global and per-VCC LANE information for the LECS configured on any interface.
Router# **show lane database** [*database-name*]	Displays the LECS database.
Router# **show lane le-arp** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*]	Displays the LE_ARP table of the LECs configured on the specified subinterface or ELAN.
Router# **show lane server** [**interface atm 0** [*subinterface-number*] | **name** *elan-name*] [**brief**]	Displays the global and per-VCC LANE information for the LES configured on a specified subinterface or ELAN.

Note For descriptions of the output displayed by the commands listed above, see the description of the command documented in the *Cisco IOS Switching Services Command Reference*.

Token Ring LANE Configuration Example

This section provides a configuration example composed of two Catalyst 5000 series switches and a Cisco LightStream 1010 ATM switch as shown in Figure 22.

Figure 22 LES/BUS and LECS Configuration



Example Assumptions

For the example in Figure 22 the following assumptions apply:

- Catalyst 5000 series switches with the ATM modules installed are running ATM software Release 4.9b or later.
- Catalyst 5000 series switch 1 runs the LES/BUS and LECS on interface **atm0** and the LEC on interface **atm0.1**.
- Catalyst 5000 series switch 2 runs LEC on interface **atm0.1**.
- The ATM module is installed in slot 4 of both Catalyst 5000 series switches.
- You can change the ELAN name by entering the **set vlan** *vlan_num* [**name** *vlan_name*] command.
- The ELAN on the switches is essentially a new TrCRF. The ELAN name is crf112 and the VLAN ID is 112.
- The parent TrBRF to the TrCRF 112 is brf400 (VLAN ID 400).

Configuring the TrCRF Example

To define the TrCRF, perform the following tasks:

Step 1 At the enable prompt, enter the following command:

```
Console> (enable) set vlan 112 name crf112 type trcrf ring 112 parent 400 mode srb
```

Step 2 To verify the configuration of the new VLAN, enter the **show vlan** command.

The output indicates that crf112 has been added and that brf400 is its parent:

```
Console> (enable) show vlan 112
VLAN Name                             Status    Mod/Ports, Vlans
---- -------------------------------- --------- ----------------------------
112  crf112                           active

VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
112  trcrf 100112     4472  400    0x112  -      -    srb      0      0

VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
112  7       7       off
Console> (enable)
```

Configuring the LES/BUS and the LEC Example

To configure the LES/BUS and LEC, perform the following tasks:

Step 1 Set up the prefix of the ATM NSAP address for the switch.

Note The LightStream 1010 ATM switch provides a default prefix.

Step 2 Start a session to the ATM module by entering the **session 4** interface configuration command. You see the following display:

```
Console> session 4
Trying ATM-4...
Connected to ATM-4.
Escape character is '^]'.
ATM>
```

Step 3 Obtain the addresses of the LES/BUS for later use by entering the **enable** router configuration command (to enable configuration mode) and the **show lane default-atm-addresses** EXEC command at the ATM prompt. You see the following display:

```
ATM> enable
ATM#
ATM# show lane default-atm-addresses interface atm0

interface ATM0:
LANE Client:        47.00918100000000061705b7701.00400BFF0010.**
LANE Server:        47.00918100000000061705b7701.00400BFF0011.**
LANE Bus:           47.00918100000000061705b7701.00400BFF0012.**
LANE Config Server: 47.00918100000000061705b7701.00400BFF0013.00
ATM#
```

Note The two asterisks (**) represent the subinterface number byte in hexadecimal.

Step 4 Using the LECS address obtained in Step 3, set the address of the default LECS in the LightStream 1010 switch by entering the **configure terminal** and **atm lecs-address-default** commands on the console of the LightStream 1010 switch. You see the following display:

```
Switch> enable
Switch#
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# atm lecs-address-default 47.00918100000000061705b7701.00400BFF0013.00 1
Switch(config)# end
Switch#
```

The commands shown in this step configure the address of the LECS in the switch. The LECS ATM NSAP address is 47.00918100000000061705b7701.00400BFF0013.00. The sequence number of this LECS address, which is 1, means it is the first LECS in this switch.

Step 5 Save the configuration to NVRAM by entering the **write memory** command, as follows:

```
ATM# write memory
```

Step 6 Start a LES/BUS pair on Catalyst 5000 series switch 1 by entering the **interface atm0** and the **lane server-bus tokenring** commands in global configuration mode. On the console of Catalyst 5000 series switch 1, enter the following commands:

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0
ATM(config-subif)# lane server-bus tokenring crf112
ATM(config-subif)# end
ATM#
```

The commands shown in this step start a LES/BUS pair and assign the ATM 0 interface to crf112. The ELAN name is **crf112**, and the interface on which this LES/BUS pair is configured is **atm0**. The ELAN name must be the same as the VLAN name assigned to the TrCRF.

Step 7 Save the configuration in NVRAM entering the **write memory** command, as follows:

```
ATM# write memory
```

Step 8 Set up the LECS database on the Catalyst 5000 series switch 1.

Enter the LES address obtained in Step 3 and replace the ** with the subinterface number of the interface on which the LES/BUS is to be configured. In this example, that number is 00. Enter the **lane database** *database_name* interface configuration command, the **name** *elan_name* **server-atm-address** *atm_address* LANE database configuration command, the **name** *elan_name* **local-seg-id** *segment_number* LANE database configuration command, and the **default-name** *elan_name* commands at the ATM prompt. You see the following display:

```
ATM# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# lane database test
ATM(lane-config-database)# name trcf-default server-atm-address
                             47.0091810000000061705b7701.00400BFF0011.00
ATM (lane-config-database) name crf112 local-seg-id 0x112
ATM(lane-config-database)# default-name crf112
ATM(lane-config-database)# exit
ATM#
```

The commands shown in this step create the LECS database. The database name is *test*. The ELAN name is **crf112**. The ELAN segment number is 112. The LES ATM NSAP address is 47.0091810000000061705b7701.00400BFF0011.00.

Note The segment number you specify for **local-seg-id** keyword must be identical to the ring number of the TrCRF. The **set vlan** command assumes that any ring number you enter is in hexadecimal. The **name** *elan-name* **local-seg-id** *segment-number* LANE database configuration command assumes that any value you enter for the **local-seg-id** keyword is in decimal unless you enter it explicitly in hexadecimal.

Step 9 Save the configuration in NVRAM by entering the **write memory** command, as follows:

```
ATM# write memory
```

Step 10 Start and bind the LECS on the Catalyst 5000 series switch 1 by entering the **interface atm0**, the **lane config database** *database_name* interface configuration command, and the **lane config auto-config-atm-address** interface configuration commands at the ATM prompt. You see the following display:

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0
ATM(config-if)# lane config database test
ATM(config-if)# lane config auto-config-atm-address
ATM(config-if)# end
ATM#
```

The commands shown in this step start the LECS. The database to use is *test*. The interface on which the LECS is configured is *atm0*.

Step 11 Save the configuration in NVRAM by entering the **write memory** command, as follows:

```
ATM# write memory
```

Step 12 Start the LEC on the Catalyst 5000 series switches 1 and 2 by entering the **interface atm0.1** command and the **lane client tokenring 112 crf112** interface configuration command in configuration mode on the consoles of switches 1 and 2. The interface on which the LEC is configured is *atm0.1*. The ELAN name is default, and it is configured to emulate Token Ring. You see the following display:

```
ATM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ATM(config)# interface atm0.1
ATM(config-subif)# lane client tokenring 112 crf112
ATM(config-subif)# end
ATM#
```

Step 13 Save the configuration in NVRAM by entering the **write memory** command, as follows:

```
ATM# write memory
```

MPOA Overview

This part consists of the following:

- Multiprotocol over ATM Overview
- MPLS Diff-Serv-aware Traffic Engineering (DS-TE) over ATM

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:

- How MPOA Works
- MPOA Components
- MPOA Components
- Configuring an MPC/MPS

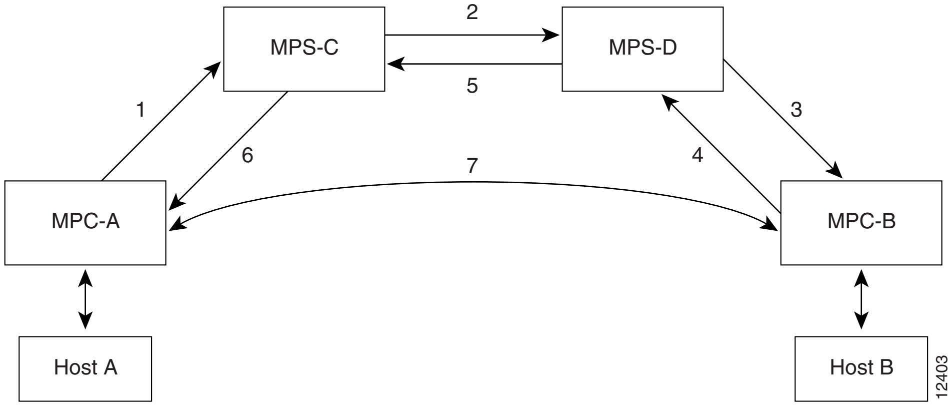
For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

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 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 23 MPOA Message Flow Between MPCs and MPSs



The sequence of events shown in Figure 23 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 16 lists and defines the MPOA terms used in Figure 23.

Table 16 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 23 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

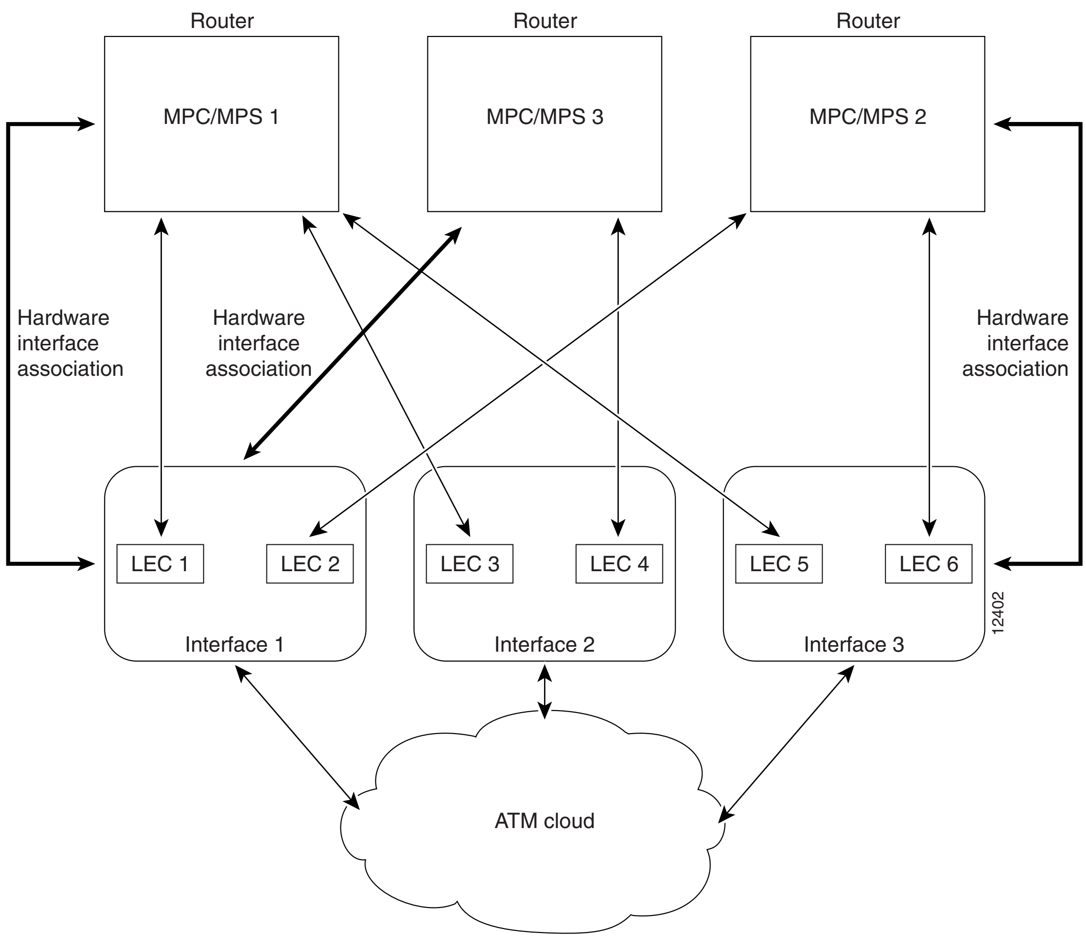
An MPOA functional network must have at least one MPS, one or more MPCs, and zero or more intermediate routers implementing NHRP servers. The MPSs and MPCs use LANE control frames to discover each other's presence in the LANE network.

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 24 shows the relationships between MPC/MPS and LECs.

Figure 24 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 24, 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.

MPLS Diff-Serv-aware Traffic Engineering (DS-TE) over ATM

This guide presents extensions made to Multiprotocol Label Switching Traffic Engineering (MPLS TE) that make it Diff-Serv aware and applicable across ATM networks. The bandwidth reservable on each link for constraint-based routing (CBR) purposes can now be managed through two bandwidth pools: a *global pool* and a *sub-pool*. The sub-pool can be limited to a smaller portion of the link bandwidth. Tunnels using the sub-pool bandwidth can then be used in conjunction with MPLS Quality of Service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network.

Caution The Fast Reroute feature of traffic engineering is not supported on ATM interfaces.

Feature History

Release	Modification
12.0(11) ST	DS-TE feature introduced.
12.0(14) ST	Support added for IS-IS Interior Gateway Protocol.
12.0(14) ST-1	Support added for guaranteed bandwidth service directed to many destination prefixes (for example, guaranteed bandwidth service destined to an autonomous system or to a BGP community).
12.2(4) T	Support added for Cisco Series 7200 platform and for ATM-PVC interface.
12.2(8) T	Support added for LC-ATM interface.

The guide contains the following sections:

Note References made to specific page numbers are meant to help readers of the printed (Acrobat™.PDF) form of this guide. On-line readers may simply click on the page number (or the underlined, colored, or bolded text) to go to the referenced page.

Background and Overview

MPLS traffic engineering allows constraint-based routing of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Diff-Serv-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of "guaranteed" traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a *sub-pool*, while the regular TE tunnel bandwidth is called the *global pool*. (The sub-pool is a portion of the global pool.) This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

For example, DS-TE can be used to ensure that traffic is routed over the network so that, on every link, there is never more than 40 per cent (or any assigned percentage) of the link capacity of guaranteed traffic (for example, voice), while there can be up to 100 per cent of the link capacity of regular traffic. Assuming QoS mechanisms are also used on every link to queue guaranteed traffic separately from regular traffic, it then becomes possible to enforce separate "overbooking" ratios for guaranteed and regular traffic. (In fact, for the guaranteed traffic it becomes possible to enforce no overbooking at all—or even an underbooking—so that very high QoS can be achieved end-to-end for that traffic, even while for the regular traffic a significant overbooking continues to be enforced.)

Also, through the ability to enforce a maximum percentage of guaranteed traffic on any link, the network administrator can directly control the end-to-end QoS performance parameters without having to rely on over-engineering or on expected shortest path routing behavior. This is essential for transport of applications that have very high QoS requirements (such as real-time voice, virtual IP leased line, and bandwidth trading), where over-engineering cannot be assumed everywhere in the network.

DS-TE involves extending OSPF (Open Shortest Path First routing protocol), so that the available sub-pool bandwidth at each preemption level is advertised in addition to the available global pool bandwidth at each preemption level. And DS-TE modifies constraint-based routing to take this more complex advertised information into account during path computation.

Benefits

Diff-Serv-aware Traffic Engineering enables service providers to perform separate admission control and separate route computation for discrete subsets of traffic (for example, voice and data traffic).

Therefore, by combining DS-TE with other IOS features such as QoS, the service provider can:

- Develop QoS services for end customers based on *signaled* rather than *provisioned* QoS
- Build the higher-revenue generating "strict-commitment" QoS services, without over-provisioning
- Offer virtual IP leased-line, Layer 2 service emulation, and point-to-point guaranteed bandwidth services including voice-trunking
- Enjoy the scalability properties offered by MPLS

Related Features and Technologies

The DS-TE feature is related to OSPF, IS-IS, RSVP (Resource reSerVation Protocol), QoS, and MPLS traffic engineering. Cisco documentation for all of these features is listed in the next section.

Related Documents

For OSPF:

- "Configuring OSPF" in Cisco IOS Release 12.1 *IP and IP Routing Configuration Guide, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdospf.htm*
- "OSPF Commands" in Cisco IOS Release 12.1 *IP and IP Routing Command Reference, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/1rdospf.htm*

For IS-IS:

- "Configuring Integrated IS-IS" in Cisco IOS Release 12.1 *IP and IP Routing Configuration Guide*, *http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdisis.htm*
- "Integrated IS-IS Commands" in Cisco IOS Release 12.1 *Cisco IOS IP and IP Routing Command Reference, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/1rdisis.htm*

For RSVP:

- "Configuring RSVP" in Cisco IOS Release 12.1 *Quality of Service Solutions Configuration Guide, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt5/qcdrsvp.htm*
- IP RSVP commands section in Cisco IOS Release 12.1 *Quality of Service Solutions Command Reference*, *http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/qrdcmd2.htm*

For QoS:

- Cisco IOS Release 12.1 *Quality of Service Solutions Configuration Guide, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/index.htm*
- Cisco IOS Release 12.1 *Quality of Service Solutions Command Reference, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/index.htm*

For MPLS Traffic Engineering:

- Cisco IOS Release 12.1(3)T *MPLS Traffic Engineering and Enhancements, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/traffeng.htm*

- "Multiprotocol Label Switching" in Cisco IOS Release 12.1 *Switching Services Configuration Guide,* *http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt4*
- Section containing MPLS commands in Cisco IOS Release 12.1 *Switching Services Command Reference,* *http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_r/xrdscmd3.htm*

For ATM:

- ATM-PVC: the "Configuring ATM" chapter of the Release 12.2 *Cisco IOS Wide-Area Networking Configuration Guide*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfatm.htm
- ATM-LSR: the "Configuring Trunks and Adding Interface Shelves" chapter of the Release 9.3.30 *BPX 8600 Series Installation and Configuration Guide*
http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/9_3_3/iandc/bpxi18.htm
and
the Release 9.3.10 *Update to the Cisco WAN Switch Command Reference Guide*
http://www.cisco.com/univercd/cc/td/doc/product/wanbu/bpx8600/9_3_1/update/udcmdref.htm

Platforms and Interfaces Supported

This release supports DS-TE together with QoS on the POS, ATM-PVC, and LC-ATM interfaces of the Cisco 7200 and 7500 Series Routers.

To carry DS-TE tunnels through an MPLS ATM cloud, an ATM-LSR should contain a Cisco 7200 router (functioning as its Label Switch Controller) and any one of the following ATM switches:

- Cisco BPX 8600, 8650, or 8680
- Cisco IGX 8410, 8420, or 8430

To check for changes in platform support since the publication of this document, access *Feature Navigator* at http://www.cisco.com/go/fn . You must have an account on Cisco.com . Qualified users can establish an account by following directions at http://www.cisco.com/register .

If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered, and account details with a new random password will then be e-mailed to you.

Supported Standards

Standardization of Diff-Serv-aware MPLS Traffic Engineering is still in progress in the IETF (Internet Engineering Task Force). At the time of publication of this feature guide, DS-TE has been documented in the following IETF drafts:

- *Requirements for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, A. Chiu, W. Townsend, D. Skalecki & M. Tatham
http://search.ietf.org/internet-drafts/draft-ietf-tewg-diff-te-reqts-nn.txt
- *Protocol Extensions for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, J. Boyle, K. Kompella, W. Townsend & D. Skalecki
http://search.ietf.org/internet-drafts/draft-ietf-tewg-diff-te-proto-01.txt

As the IETF work is still in progress, details are still under definition and subject to change, so DS-TE should be considered as a pre-standard implementation of IETF DiffServ-aware MPLS Traffic Engineering. However, it is in line with the requirements described in the first document above. The concept of "Class-Type" defined in that IETF draft corresponds to the concept of bandwidth pool implemented by DS-TE. And because DS-TE supports two bandwidth pools (global pool and sub-pool), DS-TE should be seen as supporting two Class-Types (Class-Type 0 and Class-Type 1).

Prerequisites

Your network must support the following Cisco IOS features in order to support guaranteed bandwidth services based on Diff-Serv-aware Traffic Engineering:

- MPLS
- IP Cisco Express Forwarding (CEF)
- OSPF or ISIS
- RSVP-TE
- QoS

Configuration Tasks

This section lists the minimum set of commands you need to implement the Diff-Serv-aware Traffic Engineering feature—in other words, to establish a tunnel that reserves bandwidth from the sub-pool.

The subsequent "Configuration Examples" section (page 14), presents these same commands in context and shows how, by combining them with QoS commands, you can build guaranteed bandwidth services.

New Commands

DS-TE commands were developed from the existing command set that configures MPLS traffic engineering. The only difference introduced to create DS-TE was the expansion of two commands:

- **ip rsvp bandwidth** was expanded to configure the size of the sub-pool on every link.
- **tunnel mpls traffic-eng bandwidth** was expanded to enable a TE tunnel to reserve bandwidth from the sub-pool.

The ip rsvp bandwidth command

The old command was

```
ip rsvp bandwidth x y
```

where x = the size of the only possible pool, and y = the size of a single traffic flow (ignored by traffic engineering)

Now the extended command is

```
ip rsvp bandwidth x y sub-pool z
```

where x = the size of the global pool, and z = the size of the sub-pool.

(Remember, the sub-pool's bandwidth is less than—because it is part of—the global pool's bandwidth.)

The tunnel mpls traffic-eng bandwidth command

The old command was

```
tunnel mpls traffic-eng bandwidth b
```

where b = the amount of bandwidth this tunnel requires.

Now you specify from which pool (global or sub) the tunnel's bandwidth is to come. You can enter

```
tunnel mpls traffic-eng bandwidth sub-pool b
```

This indicates that the tunnel should use bandwidth from the sub-pool. Alternatively, you can enter

```
tunnel mpls traffic-eng bandwidth b
```

This indicates that the tunnel should use bandwidth from the global pool (the default).

Note As can be seen in the Guaranteed Bandwidth Service Examples section (page 24), when QoS commands are added to DS-TE commands, guaranteed bandwidth tunnels can be created. To accomplish that across an MPLS ATM cloud, two more commands were created (beginning with Release 12.2(8)T): **mpls traffic-eng atm cos global-pool** and **mpls traffic-eng atm cos sub-pool**.

The Configuration Procedure

To establish a sub-pool TE tunnel, you must enter configurations at three levels:

- the device (router, switch router, or label switch router)
- the physical interface (network interface)
- the tunnel interface

On the first two levels, you activate traffic engineering (and certain ATM settings if the tunnel will cross an ATM cloud). On the third level—the tunnel interface—you establish the sub-pool tunnel. Therefore, it is only at the tunnel headend device that you need to configure all three levels. At the tunnel midpoints and tail, it is sufficient to configure the first two levels.

In the tables below, each command is explained in brief. For a more complete explanation of any command, refer to the page given in the right-hand column.

Level 1: Configuring the Device

At this level, you tell the device (router or switch router) to use accelerated packet-forwarding (known as Cisco Express Forwarding or CEF), MultiProtocol Label Switching (MPLS), traffic-engineering tunneling, and either the OSPF or IS-IS routing algorithm (Open Shortest Path First or Intermediate

System to Intermediate System). This level is often called global configuration mode because the configuration is applied globally, to the entire device, rather than to a specific interface or routing instance.

You enter the following commands:

	Command	Purpose
Step 1	`Router(config)# ip cef`	Enables CEF—which accelerates the flow of packets through the device.
Step 2	`Router(config)# mpls traffic-eng tunnels`	Enables MPLS, and specifically its traffic engineering tunnel capability.
Step 3	`Router(config)# mpls traffic-eng atm cos sub-pool`	[To be used only on ATM-LSR devices that are midpoints of a DS-TE tunnel]. Maps the queue carrying sub-pool traffic onto the highest cell-based class of service.
	`Router(config)# mpls traffic-eng atm cos global-pool`	(Optional). Maps the queue carrying global pool traffic onto one of the remaining three classes of service.
Step 4	`Router(config)# router ospf`	Invokes the OSPF routing process for IP and puts the device into router configuration mode. Proceed now to Steps 10and 11.
	`[or]` `Router(config)# router isis`	Alternatively, you may invoke the ISIS routing process with this command and continue with Step 5.
Step 5	`Router (config-router)# net` *network-entity-title*	Specifies the IS-IS network entity title (NET) for the routing process.
Step 6	`Router (config-router)# metric-style wide`	Enables the router to generate and accept IS-IS new-style TLVs (type, length, and value objects).
Step 7	`Router (config-router)# is-type level-`*n*	Configures the router to learn about destinations inside its own area or “IS-IS level”.
Step 8	`Router (config-router)# mpls traffic-eng level-`*n*	Specifies the IS-IS level (which must be the same level as in the preceding step) to which the router will flood MPLS traffic-engineering link information.
Step 9	`Router (config-router)# passive-interface loopback0`	Instructs IS-IS to advertise the IP address of the loopback interface without actually running IS-IS on that interface. Continue with Step 10 but don’t do Step 11—because Step 11 refers to OSPF.
Step 10	`Router(config-router)# mpls traffic-eng router-id loopback0`	Specifies that the traffic engineering router identifier is the IP address associated with the *loopback0* interface.
Step 11	`Router(config-router)# mpls traffic-eng area` *num*	Turns on MPLS traffic engineering for a particular OSPF area.

Level 2: Configuring the Network Interface

Having configured the device, you now must configure the interface on that device through which the tunnel will run. To do that, you first put the router into interface-configuration mode.

You then enable Resource Reservation Protocol (RSVP). RSVP is used to signal (set up) a traffic engineering tunnel, and to tell devices along the tunnel path to reserve a specific amount of bandwidth for the traffic that will flow through that tunnel. It is with this command that you establish the maximum size of the sub-pool.

Finally, you enable the MPLS traffic engineering tunnel feature on this network interface—and if you will be relying on the IS-IS routing protocol, you enable that as well. (In the case of ATM-PVC and LC-ATM interfaces you must enable IS-IS on a *sub*-interface level, and you must enable MPLS on *both* the interface and the sub-interface levels.)

To accomplish these tasks, you enter the following commands. (Step 7 or 8 is entered only when the interface you are configuring is either an ATM-PVC – Step 7 – or an LC-ATM – Step 8).

	Command	Purpose
Step 1	`Router(config)#` **`interface`** *`interface-id`*	Moves configuration to the interface level, directing subsequent configuration commands to the specific interface identified by the *interface-id*.
Step 2	`Router(config-if)#` **`ip rsvp bandwidth`** *`interface-kbps`* **`sub-pool`** *`kbps`*	Enables RSVP on this interface and limits the amount of bandwidth RSVP can reserve on this interface. The sum of bandwidth used by all tunnels on this interface cannot exceed *interface-kbps,* and the sum of bandwidth used by all sub-pool tunnels cannot exceed sub-pool *kbps*.
Step 3	`Router(config-if)#` **`mpls traffic-eng tunnels`**	Enables the MPLS traffic engineering tunnel feature on this interface. If the tunnel will go through an ATM-PVC or LC-ATM interface, continue on through Steps 4 through 11. However, if the tunnel will go through a POS interface, skip immediately to Step 11.
Step 4	`Router(config-if)#` **`interface`** *`interface-id.int-sub`* **`[mpls]`**	Moves configuration to the sub-interface level, directing subsequent configuration commands to the specific sub-interface identified by the *interface-id.sub-int*. Needed when the tunnel will traverse an ATM-PVC or LC-ATM interface. The keyword **mpls** is needed only with the LC-ATM interface.
Step 5	`Router(config-subif)#` **`ip rsvp bandwidth`** *`interface-kbps`* **`sub-pool`** *`kbps`*	Enables RSVP on the sub-interface and limits the amount of bandwidth RSVP can reserve on the sub-interface. The sum of bandwidth used by all tunnels on this sub-interface cannot exceed *interface-kbps,* and the sum of bandwidth used by all sub-pool tunnels cannot exceed sub-pool *kbps*.
Step 6	`Router(config-subif)#` **`mpls traffic-eng tunnels`**	Enables the MPLS traffic engineering tunnel feature on this sub-interface. If interface is ATM-PVC, continue with Step 7. If instead the interface is LC-ATM, skip to Step 8.]
Step 7	`Router(config-subif)#` **`atm pvc`** *`vcd vpi vci aal5snap`*	Sets the ATM PVC descriptor, path identifier, and channel identifier. Also sets the encapsulation as AAL5SNAP. [Now skip ahead to Step 9.]
Step 8	`Router(config-subif)#` **`mpls atm`** *`vpi`*-*`vpi`*	Sets the range of Virtual Path Identifiers on the LC-ATM interface.
Step 9	`Router(config-subif)#` **`ip router isis`**	Enables the IS-IS routing protocol on the sub-interface. Do not enter this command if you are configuring for OSPF.
Step 10	`Router(config-subif)#` **`exit`**	Exits the sub-interface level, returning to the interface level.
Step 11	`Router(config-if)#` **`ip router isis`**	If you are configuring an interface that does not have sub-interfaces, like POS, you enable IS-IS routing protocol at this step, on the interface level. (More on page 68.) Do not enter this command if you are configuring for OSPF.

Level 3: Configuring the Tunnel Interface

Now you create a set of attributes for the tunnel itself; those attributes are configured on the "tunnel interface" (not to be confused with the network interface just configured above).

The only command at this level which was affected to create DS-TE is **tunnel mpls traffic-eng bandwidth** (described in detail on page 145).

You enter the following commands:

	Command	Purpose
Step 1	`Router(config)#` **`interface tunnel1`**	Creates a tunnel interface (named in this example **tunnel1**) and enters interface configuration mode. (More on page 62.)
Step 2	`Router(config-if)#` **`tunnel destination`** *`A.B.C.D`*	Specifies the IP address of the tunnel tail device. (More on page 139.)
Step 3	`Router(config-if)#` **`tunnel mode mpls traffic-eng`**	Sets the tunnel's encapsulation mode to MPLS traffic engineering. (More on page 141.)
Step 4	`Router(config-if)#` **`tunnel mpls traffic-eng bandwidth`** `{`**`sub-pool`** `|` `[`**`global`**`]}` *`bandwidth`*	Configures the tunnel's bandwidth and assigns it either to the sub-pool or the global pool. (More on page 145).
Step 5	`Router(config-if)#` **`tunnel mpls traffic-eng priority`**	Sets the priority to be used when system determines which existing tunnels are eligible to be preempted. (More on page 148).
Step 6	`Router(config-if)#` **`tunnel mpls traffic-eng path-option`**	Configures the paths (hops) a tunnel should use. The user can enter an explicit path (can specify the IP addresses of the hops) or can specify a dynamic path (the router figures out the best set of hops). (More on page 147).

ATM-LSR Special Case

Because of the joint nature of the ATM-LSR device—being both a router running Cisco IOS and an ATM switch running its own, different operating system—distinct configuration tasks are required to have this device convey DS-TE tunnels across itself as a tunnel midpoint. (The ATM-LSR device cannot be the head nor tail of a DS-TE tunnel, only a midpoint).

Configuring the ATM-LSR midpoint device thus involves four tasks:

- Configuring a link between the router portion of the device and the switch portion
- Mapping router-level traffic pools to switch-level classes of service
- Mapping logical interfaces on the router to physical ports on the switch (the results are called XTagATM interfaces)
- Configuring resources within the switch (using the switch's own command language to address its operating system, different from Cisco IOS).

Establishing a link between the router portion and the switch's control port

	Command	Purpose
Step 1	`Router(config)#` **`interface atm4/1 0/0/0`**	Moves configuration to the interface level, directing subsequent configuration commands to a Virtual Switch Interface on the router portion of the device. (More on page 62.)
Step 2	`Router(config-if)#` **`label-control-protocol vsi`**	Enables Virtual Switch Interface protocol as the means of communication between the router interface and the switch's control port.

Mapping pools to classes of service

	Command	Purpose
Step 1	`Router(config)#` **`mpls traffic-eng atm cos sub-pool`**	Directs all sub-pool traffic entering the ATM-LSR to exit as the highest priority ATM class of service. (More on page 78.)
Step 2	`Router(config)#` **`mpls traffic-eng atm cos global-pool`** `[available | standard | premium]`	(Optional). Directs all global pool traffic entering the ATM-LSR to exit as one of the remaining three classes of service. (More on page 77.) If you don't use this command, the default, lowest priority service—"**available**"—is assigned.

Mapping switch ports to XTag-ATM interfaces, and configuring those interfaces

	Command	Purpose
Step 1	`Router(config)#` **`interface Xtagatm22`**	Moves configuration to the interface level, directing subsequent configuration commands to the specified XTag-ATM interface. (More on page 62.)
Step 2	`Router(config-if)#` **`extended-port atm4/1 0/0/0 bpx2.2`**	Associates a port on the switch with this XTagATM interface. **extended-port** *ctrl-if* {**bpx***port.number* | **igx***port.number* | **descriptor** *vsi-descriptor* | **vsi** *vsi-port-numbe*r}
Step 3	`Router(config-if)#` **`ip address 10.1.1.2 255.0.0.0`**	Gives a network IP address to the XTagATM interface.
Step 4	`Router(config-if)#` **`ip rsvp bandwidth`** *`interface-kbps`* **`sub-pool`** *`kbps`*	Enables RSVP on the XTagAtm interface and limits the amount of bandwidth RSVP can reserve on the interface. The sum of bandwidth used by all tunnels on this interface cannot exceed *interface-kbps,* and the sum of bandwidth used by all sub-pool tunnels cannot exceed sub-pool *kbps*. (More on page 69.)
Step 5	`Router(config-if)#` **`mpls traffic-eng tunnels`**	Enables the MPLS traffic engineering tunnel feature on this interface. (More on page 88.)

	Command	Purpose
Step 6	`Router(config-if)#` **`mpls atm`** *`vpi`*`-`*`vpi`*	Sets the range of Virtual Path Identifiers on this interface. (More on page 138.)
Step 7	`Router(config-if)#` **`ip router isis`**	Enables the IS-IS routing protocol on this interface. (More on page 68.) Do not enter this command if you are configuring for OSPF.

Configuring resources within the switch

(Reminder—the following commands are entered directly into the switch. They are not part of the router portion's Cisco IOS software.)

	Command	Purpose
Step 1	`BPX-12#` **`uptrk`** *`slot.port[.vtrk]`*	Activates a trunk, to generate framing. (The optional virtual trunk specification—*vrtk*— is not used in our example).
Step 2	`BPX-12#` **`addshelf`** *`slot.port.`* **`v`** *`slot.port.`*	Creates an interface shelf, to drive ATM cells to and from the switch.
Step 3	`BPX-12#` **`cnfrsrc`** *`slot.port.vtrk maxpvclcns maxpvcbw y/n partition e/d minvsilcns maxvsilcns vsistartvpi vsiendvpi vsiminbw vsimaxbw`*	Configures resources for ports and trunks.

Verifying the Configurations

To view the complete configuration you have entered, use the EXEC command **show running-config** and check its output display for correctness.

To check *just one tunnel*'s configuration, enter **show interfaces tunnel** followed by the tunnel interface number. And to see that tunnel's RSVP bandwidth and flow, enter **show ip rsvp interface** followed by the name or number of the network interface (and also, in the case of an ATM-PVC or LC-ATM interface, the name or number of the sub-interface).

Here is an example of the information displayed by these two commands. To see an explanation of each field used in the following displays turn to page 95 for **show interfaces tunnel** and page 109 for **show ip rsvp interface**.

```
RTR1#show interfaces tunnel 4
Tunnel4 is up, line protocol is down
  Hardware is Routing Tunnel
  MTU 1500 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set, keepalive set (10 sec)
  Tunnel source 0.0.0.0, destination 0.0.0.0
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
```

```
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets, 0 restarts

RTR1#show ip rsvp interface pos4/0
interface    allocated  i/f max  flow max sub max
PO4/0        300K       466500K  466500K  0M

RTR1#show ip rsvp interface atm3/0
RTR1#show ip rsvp interface atm3/0.5
interface    allocated  i/f max  flow max sub max
AT3/0.5 110M 130M 130M 100
```

To view *all tunnels at once* on the router you have configured, enter **show mpls traffic-eng tunnels brief**. The information displayed when tunnels are functioning properly looks like this (a table explaining the display fields begins on page 136):

```
RTR1#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 3029 seconds
TUNNEL NAME DESTINATION      UP IF     DOWN IF   STATE/PROT
RTR1_t0 192.168.1.13     -         SR3/0     up/up
RTR1_t1 192.168.1.13     -         SR3/0     up/up
RTR1_t2 192.168.1.13     -         PO4/0     up/up
[[RTR1_t3 192.168.1.13     -         AT3/0.5 up/up]]
Displayed 4(of 4) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

When one or more tunnels are not functioning properly, the display could instead look like this. (In the following example, tunnels t0 and t1 are down, as indicated in the far right column).

```
RTR1#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 2279 seconds
TUNNEL NAME DESTINATION      UP IF     DOWN IF   STATE/PROT
RTR1_t0 192.168.1.13     -         SR3/0     up/down
RTR1_t1 192.168.1.13     -         SR3/0     up/down
RTR1_t2 192.168.1.13     -         PO4/0     up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

To find out *why* a tunnel is down, insert its name into this same command, after adding the keyword **name** and omitting the keyword **brief**. For example:

```
RTR1#show mpls traffic-eng tunnels name RTR1_t0
Name:RTR1_t0                            (Tunnel0) Destination:192.168.1.13
  Status:
    Admin:up         Oper:down Path: not valid       Signalling:connected
```

If, as in this example, the Path is displayed as **not valid**, use the **show mpls traffic-eng topology** command to make sure the router has received the needed updates. (That command is described on page 133.)

Additionally, you can use any of the following **show** commands to inspect particular aspects of the network, router, or interface concerned:

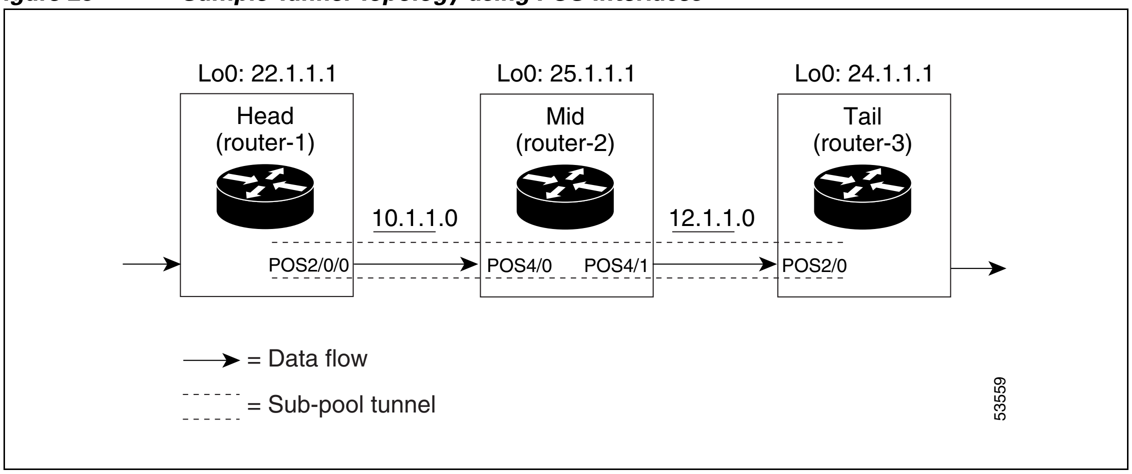
To see information about...		
this level	**and this item...**	**Use this command**
Network	Advertised bandwidth allocation information	**show mpls traffic-eng link-management advertisements** (described on page 121)
	Preemptions along the tunnel path	**debug mpls traffic-eng link-management preemption** (described on page 61)
	Available TE link bandwidth on all head routers	**show mpls traffic-eng topology** (described on page 133)
Router	Status of all tunnels currently signalled by this router	**show mpls traffic-eng link-management admission-control** (described on page 119)
	Tunnels configured on midpoint routers	**show mpls traffic-eng link-management summary** (described on page 131)
Interface	Detailed information on current bandwidth pools	**show mpls traffic-eng link-management bandwidth-allocation [interface-name]** (described on page 124
	TE RSVP bookkeeping	**show mpls traffic-eng link-management interfaces** (described on page 129)
	Entire configuration of one interface	**show run interface**

Configuration Examples

First this section presents the DS-TE configurations needed to create the sub-pool tunnel. Then it presents the more comprehensive design for building end-to-end guaranteed bandwidth service, which involves configuring Quality of Service as well.

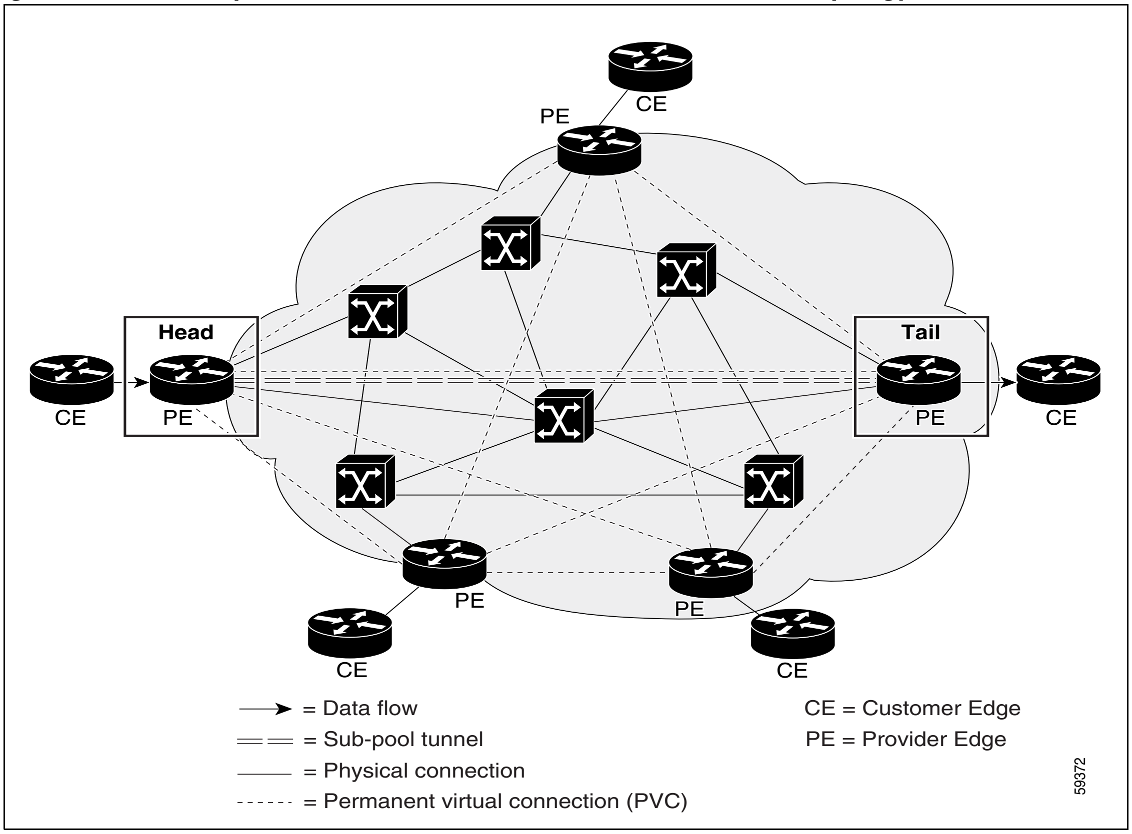
As shown in Figure 1, the tunnel configuration involves at least three devices—tunnel head, midpoint, and tail. On each of those devices one or two network interfaces must be configured, for traffic ingress and egress.

Figure 25 Sample Tunnel Topology using POS Interfaces



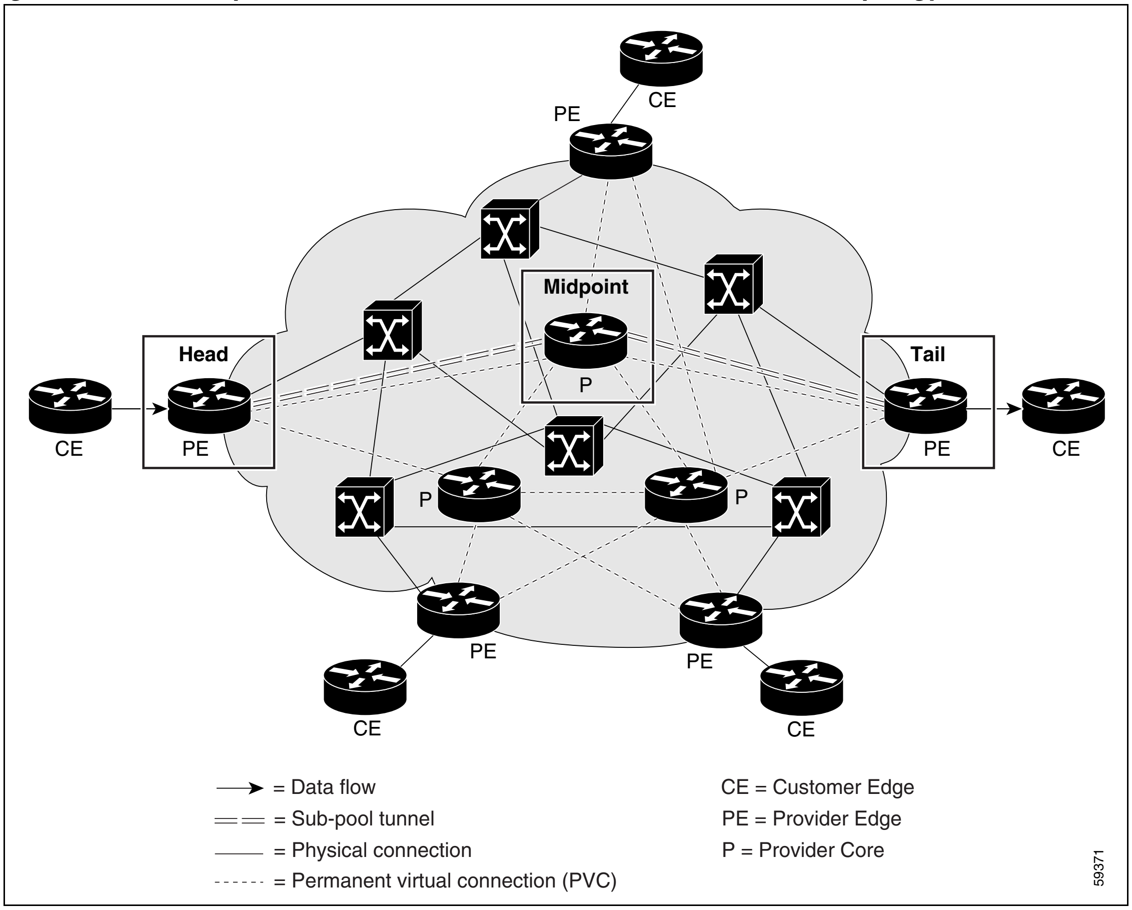
Sample topologies when the tunnel will run over ATM-PVCs are shown in Figure 2 (full mesh) and Figure 3 (partial mesh). A sample topology for tunnels that traverse LC-ATM interfaces is shown in Figure 4.

Figure 26 Sample Tunnel across ATM-PVC Interfaces -- Full Mesh Topology



The full mesh topology shows no Midpoint device because the sub-pool tunnel can be routed along a direct PVC connecting the Head and Tail devices. However, if that particular PVC does not contain enough bandwidth, the tunnel can pass through alternate PVCs which may connect one or more PE routers. In that case the alternate PE router(s) will function as tunnel midpoint(s), and must be configured as shown in the Midpoint sections of the following configuration examples.

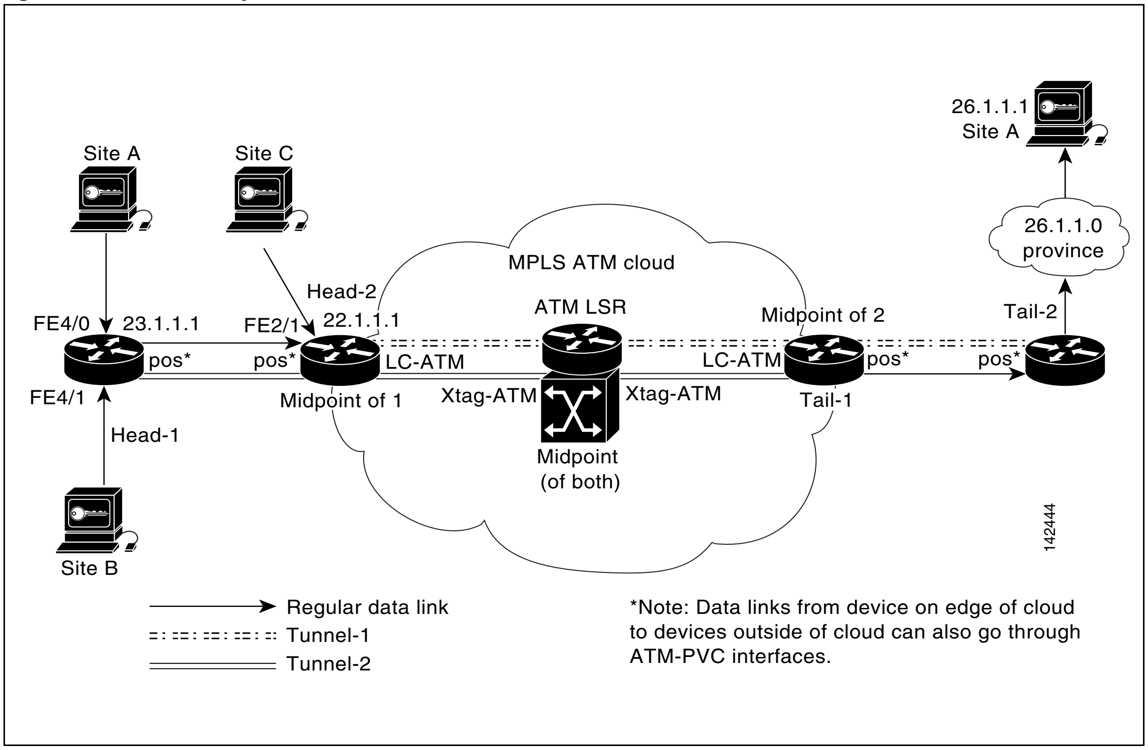
Figure 27 Sample Tunnel across ATM-PVC Interfaces -- Partial Mesh Topology



As shown in Figure 4, DS-TE tunnels that travel through an MPLS ATM cloud can start either at a device outside the cloud or at one located on the edge of the cloud. Likewise, these tunnels can end either at a device on the edge of the cloud or one that is wholly outside the cloud. However, DS-TE tunnels cannot begin or end *inside* an MPLS ATM cloud.

On the edge of the cloud, the interface conveying the tunnel is an LC-ATM. Within the cloud, it is an XTag-ATM, residing on an ATM-LSR device.

Figure 28 Sample Tunnels across LC-ATM Interfaces



The following example refers to all three figures. Where the language is specific to only one type of interface, that fact is indicated.

Tunnel Head

At the device level:

```
router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

router(config)# ip cef
router(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

`router(config)# router isis`	`router ospf 100`
`router(config-router)# net 49.0000.1000.0000.0010.00`	`redistribute connected`
`router(config-router)# metric-style wide`	`network 10.1.1.0 0.0.0.255 area 0`
`router(config-router)# is-type level-1`	`network 22.1.1.1 0.0.0.0 area 0`
`router(config-router)# mpls traffic-eng level-1`	`mpls traffic-eng area 0`
`router(config-router)# passive-interface Loopback0`	

[now one resumes the common command set]:

```
router(config-router)# mpls traffic-eng router-id Loopback0
```

```
    router(config-router)# exit

router(config)# interface Loopback0
```

At the virtual interface level:

```
    router(config-if)# ip address 22.1.1.1 255.255.255.255
    router(config-if)# no ip directed-broadcast
    router(config-if)# exit
```

At the device level:
[ATM cases appear on the left; POS case on the right]:

```
router(config)# interface atm3/0
```

[continuing each case at the network interface level (egress)]:

```
router(config-if)# mpls traffic-eng tunnels
router(config-if)# ip rsvp bandwidth 130000 130000/
                   sub-pool 80000
router(config-if)# interface atm3/0.5
```

[append the keyword mpls if LC-ATM]

```
router(config-subif)# ip address 10.1.1.1
                   255.255.255.0
router(config-subif)#ip rsvp bandwidth 130000 130000
                   sub-pool 80000
router(config-subif)# mpls traffic-eng tunnels
router(config-subif)#
```

[if ATM-PVC] : atm pvc 10 10 100 aal5snap
[if LC-ATM] : mpls atm vpi 2-5
[if using IS-IS instead of OSPF]:

```
router(config-subif)# ip router isis
router(config-subif)# exit
router(config-if)#
```

POS case:

```
interface POS2/0/0
ip address 10.1.1.1 255.255.255.0
mpls traffic-eng tunnels
ip rsvp bandwidth 130000 130000/
   sub-pool 80000
```

[If using IS-IS instead of OSPF]:

```
ip router isis
```

Continuing at the network interface level, regardless of interface type:

```
router(config-if)# exit
```

At the device level:

```
router(config)# interface Tunnel1
```

At the tunnel interface level:

```
    router(config-if)# bandwidth 110000
    router(config-if)# ip unnumbered Loopback0
    router(config-if)# tunnel destination 24.1.1.1
    router(config-if)# tunnel mode mpls traffic-eng
    router(config-if)# tunnel mpls traffic-eng priority 0 0
    router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
    router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
    router(config-if)# exit
router(config)#
```

Midpoint Devices

At the device level:

```
router# configure terminal
```

```
router(config)# ip cef
router(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router(config)# **router isis**	**router ospf 100**
router(config-router)# **net 49.0000.1000.0000.0012.00**	**redistribute connected**
router(config-router)# **metric-style wide**	**network 11.1.1.0 0.0.0.255 area 0**
router(config-router)# **is-type level-1**	**network 12.1.1.0 0.0.0.255 area 0**
router(config-router)# **mpls traffic-eng level-1**	**network 25.1.1.1 0.0.0.0 area 0**
router(config-router)# **passive-interface Loopback0**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router(config-router)# mpls traffic-eng router-id Loopback0
router(config-router)# exit
```

```
router(config)# interface Loopback0
```

At the virtual interface level:

```
router(config-if)# ip address 25.1.1.1 255.255.255.255
router(config-if)# no ip directed-broadcast
router(config-if)# exit
```

[And if the device is an ATM-LSR:

```
router(config)#interface atm9/0 0/0/0
router(config-if)# label-control-protocol vsi
router(config-if)# exit
router(config)#mpls traffic-eng atm cos sub-pool
```
]

On all devices, for the ingress interface:
[ATM-LSR appears on the left; ATM-PVC and LC-ATM cases in the middle; POS on the right]

router(config)# **interface Xtagatm22**	**interface atm3/0**	**interface POS4/0**

[continuing each case at the network interface level]

router(config-if)# **extended-port atm9/0 bpx2.2**	**mpls traffic-eng tunnels**	**ip address 11.1.1.2 255.255.255.0**
router(config-if)# **ip address 11.1.1.2 255.255.255.0**	**ip rsvp bandwidth 130000 130000/ sub-pool 80000**	**mpls traffic-eng tunnels**
router(config-if)# **ip rsvp bandwidth 130000 130000 sub-pool 80000**		**ip rsvp bandwidth 130000 130000/ sub-pool 80000**
router(config-if)# **mpls traffic-eng tunnels**		[If using IS-IS instead of OSPF]: **ip router isis**
router(config-if)# **mpls atm vpi 2-15**		
router(config-if)# **ip rsvp isis** [only if using IS-IS instead of OSPF]	**interface atm3/0.5** [append the keyword **mpls** if LC-ATM]	
router(config-subif)#	**ip address 11.1.1.2 255.255.255.0**	
router(config-subif)#	**ip rsvp bandwidth 130000 130000 sub-pool 80000**	
router(config-subif)#	**mpls traffic-eng tunnels**	
router(config-subif)#	[if ATM-PVC] : **atm pvc 10 10 100 aal5snap** [or if LC-ATM] : **mpls atm vpi 2-15**	
router(config-subif)#	[If using IS-IS instead of OSPF]: **ip router isis**	
router(config-subif)#	**exit**	

Continuing at the network interface level, regardless of interface type:

```
router(config-if)# exit
```

At the device level, for the egress interface:
[ATM-LSR appears on the left; ATM-PVC and LC-ATM cases in the middle; POS on the right]

router(config)# **interface Xtagatm44**	**interface atm4/0**	**interface POS4/1**

[continuing each case at the network interface level]

router(config-if)# **extended-port atm9/0 bpx4.4**	**mpls traffic-eng tunnels**	**ip address 12.1.1.2 255.255.255.0**
router(config-if)# **ip address 12.1.1.2 255.255.255.0**	**ip rsvp bandwidth 130000 130000/ sub-pool 80000**	**mpls traffic-eng tunnels**
router(config-if)# **ip rsvp bandwidth 130000 130000 sub-pool 80000**		**ip rsvp bandwidth 130000 130000/ sub-pool 80000**
router(config-if)# **mpls traffic-eng tunnels**		[If using IS-IS instead of OSPF]: **ip router isis**
router(config-if)# **mpls atm vpi 2-15**		
router(config-if)# **ip router isis** [only if using IS-IS instead of OSPF]	**interface atm4/0.5** [append the keyword **mpls** if LC-ATM]	
router(config-subif)#	**ip address 12.1.1.2 255.255.255.0**	
router(config-subif)#	**ip rsvp bandwidth 130000 130000 sub-pool 80000**	
router(config-subif)#	**mpls traffic-eng tunnels**	
router(config-subif)#	[if ATM-PVC] : **atm pvc 10 10 100 aal5snap** [or if LC-ATM] : **mpls atm vpi 2-15**	
router(config-subif)#	[If using IS-IS instead of OSPF]: **ip router isis**	
router(config-subif)#	**exit**	

Continuing at the network interface level, regardless of interface type:

```
router(config-if)# exit
```

Note that there is no configuring of tunnel interfaces at the mid-point devices, only network interfaces, sub-interfaces, and the device globally.

When the midpoint device is an ATM-LSR, the following commands are also required. They are entered directly into the switch device, bypassing Cisco IOS:

```
BPX-12# uptrk 1.1
BPX-12# addshelf 1.1 v 1.1
BPX-12# cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
BPX-12# uptrk 2.2
BPX-12# cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000
BPX-12# uptrk 3.3
BPX-12# cnfrsrc 3.3 256 252207 y 1 e 512 4096 2 5 26000 100000
BPX-12# uptrk 4.4
BPX-12# cnfrsrc 4.4 256 252207 y 1 e 512 4096 2 5 26000 100000
BPX-12# uptrk 5.5
BPX-12# cnfrsrc 5.5 256 252207 y 1 e 512 4096 2 5 26000 100000
```

Tail-End Device

At the device level:

```
router# configure terminal
router(config)# ip cef
router(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

`router(config)# router isis`	`router ospf 100`
`router(config-router)# net 49.0000.1000.0000.0013.00`	`redistribute connected`
`router(config-router)# metric-style wide`	`network 12.1.1.0 0.0.0.255 area 0`
`router(config-router)# is-type level-1`	`network 24.1.1.1 0.0.0.0 area 0`
`router(config-router)# mpls traffic-eng level-1`	`mpls traffic-eng area 0`
`router(config-router)# passive-interface Loopback0`	

[now one resumes the common command set]:

```
router(config-router)# mpls traffic-eng router-id Loopback0
router(config-router)# exit

router(config)# interface Loopback0
```

At the virtual interface level:

```
router(config-if)# ip address 24.1.1.1 255.255.255.255
router(config-if)# no ip directed-broadcast
```

[and if using IS-IS instead of OSPF]:

```
router(config-if)# ip router isis
```

[and in all cases]:

```
router(config-if)# exit
```

At the device level:
[ATM cases appear on the left; POS case on the right]:

`router(config)# interface atm2/0`	`interface POS2/0/0`

[continuing each case at the network interface level (ingress)]:

`router(config-if)# mpls traffic-eng tunnels`	`ip address 12.1.1.3 255.255.255.0`
`router(config-if)# ip rsvp bandwidth 130000 130000/ sub-pool 80000`	`mpls traffic-eng tunnels`
`router(config-if)# interface atm2/0.4` [append the keyword `mpls` if LC-ATM]	`ip rsvp bandwidth 130000 130000/ sub-pool 80000`
`router(config-subif)# ip address 12.1.1.3 255.255.255.0`	
`router(config-subif)#ip rsvp bandwidth 130000 130000 sub-pool 80000`	
`router(config-subif)# mpls traffic-eng tunnels`	
`router(config-subif)#` [if ATM-PVC] : `atm pvc 10 10 100 aal5snap` [if LC-ATM] : `mpls atm vpi 2-5`	
[if using IS-IS instead of OSPF]:	
`router(config-subif)# ip router isis`	
`router(config-subif)# exit`	
`router(config-if)#`	[If using IS-IS instead of OSPF]: `ip router isis`

Continuing at the network interface level, regardless of interface type:

```
router(config-if)# exit
```

Guaranteed Bandwidth Service Configuration

Having configured two bandwidth pools, you now can

- Use one pool, the sub-pool, for tunnels that carry traffic requiring strict bandwidth guarantees or delay guarantees
- Use the other pool, the global pool, for tunnels that carry traffic requiring only Differentiated Service.

Having a separate pool for traffic requiring strict guarantees allows you to limit the amount of such traffic admitted on any given link. Often, it is possible to achieve strict QoS guarantees only if the amount of guaranteed traffic is limited to a portion of the total link bandwidth.

Having a separate pool for other traffic (best-effort or diffserv traffic) allows you to have a separate limit for the amount of such traffic admitted on any given link. This is useful because it allows you to fill up links with best-effort/diffserv traffic, thereby achieving a greater utilization of those links.

Providing Strict QoS Guarantees Using DS-TE Sub-pool Tunnels

A tunnel using sub-pool bandwidth can satisfy the stricter requirements if you do all of the following:

1. Select a queue—or in diffserv terminology, select a PHB (per-hop behavior)—to be used exclusively by the strict guarantee traffic. This shall be called the "GB queue."

   If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. On the Cisco 7200 it is the "priority" queue. You must configure the bandwidth of the queue to be at least equal to the bandwidth of the sub-pool.

   If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used. On the Cisco 7200 you use one of the existing Class-Based Weighted Fair Queuing (CBWFQ) queues.

2. Ensure that the guaranteed traffic sent through the sub-pool tunnel is placed in the GB queue *at the outbound interface of every tunnel hop*, and that no other traffic is placed in this queue.

   You do this by marking the traffic that enters the tunnel with a unique value in the mpls exp bits field, and steering only traffic with that marking into the GB queue.

3. Ensure that this GB queue is never oversubscribed; that is, see that no more traffic is sent into the sub-pool tunnel than the GB queue can handle.

   You do this by rate-limiting the guaranteed traffic before it enters the sub-pool tunnel. The aggregate rate of all traffic entering the sub-pool tunnel should be less than or equal to the bandwidth capacity of the sub-pool tunnel. Excess traffic can be dropped (in the case of delay/jitter guarantees) or can be marked differently for preferential discard (in the case of bandwidth guarantees).

4. Ensure that the amount of traffic entering the GB queue is limited to an appropriate percentage of the total bandwidth of the corresponding outbound link. The exact percentage to use depends on several factors that can contribute to accumulated delay in your network: your QoS performance objective, the total number of tunnel hops, the amount of link fan-in along the tunnel path, burstiness of the input traffic, and so on.

   You do this by setting the sub-pool bandwidth of each outbound link to the appropriate percentage of the total link bandwidth (that is, by adjusting the z parameter of the **ip rsvp bandwidth** command).

Providing Differentiated Service Using DS-TE Global Pool Tunnels

You can configure a tunnel using global pool bandwidth to carry best-effort as well as several other classes of traffic. Traffic from each class can receive differentiated service if you do all of the following:

1. Select a separate queue (a distinct diffserv PHB) for each traffic class. For example, if there are three classes (gold, silver, and bronze) there must be three queues (diffserv AF2, AF3, and AF4). [If the tunnel is to cross an MPLS ATM cloud, only one class of global pool traffic may be configured.]
2. Mark each class of traffic using a unique value in the MPLS experimental bits field (for example gold = 4, silver = 5, bronze = 6). [On the ATM-LSR, you specify the class of service desired **—premium**, **standard**, or the default service, **available**—using the command **mpls traffic-eng atm cos global-pool**].
3. Ensure that packets marked as Gold are placed in the gold queue, Silver in the silver queue, and so on. The tunnel bandwidth is set based on the expected aggregate traffic across all classes of service.

To control the amount of diffserv tunnel traffic you intend to support on a given link, adjust the size of the global pool on that link.

Providing Strict Guarantees and Differentiated Service in the Same Network

Because DS-TE allows simultaneous constraint-based routing of sub-pool and global pool tunnels, strict guarantees and diffserv can be supported simultaneously in a given network.

Guaranteed Bandwidth Service Examples

Given the many topologies in which Guaranteed Bandwidth Services can be applied, there is space here only to present two examples. They illustrate opposite ends of the spectrum of possibilities.

In the first example, the guaranteed bandwidth tunnel can be easily specified by its destination. So the forwarding criteria refer to a single destination prefix.

In the second example, there can be many final destinations for the guaranteed bandwidth traffic, including a dynamically changing number of destination prefixes. So the forwarding criteria are specified by Border Gateway Protocol (BGP) policies.

Example with Single Destination Prefix

Figure 5 , Figure 6, and Figure 7 illustrate topologies for guaranteed bandwidth services whose destination is specified by a single prefix. In Figure 5 the interfaces to be configured are POS (Packet over SONET), while in Figure 6 the interfaces are ATM-PVC (Asynchronous Transfer Mode – Permanent Virtual Circuit), and in Figure 7 they are LC-ATM (Label Controlled - Asynchronous Transfer Mode) and, within the MPLS ATM cloud, XTag-ATM. In all three illustrations, the destination for the guaranteed bandwidth service is either a single host (like a voice gateway, here designated “Site D” and bearing prefix 26.1.1.1) or a subnet (like a web farm, here called “Province” and bearing prefix 26.1.1.0). Three services are offered in each sample topology:

- From Site A (defined as all traffic arriving at interface FE4/0): to host 26.1.1.1, 8 Mbps of guaranteed bandwidth with low loss, low delay and low jitter
- From Site B (defined as all traffic arriving at interface FE4/1): towards subnet 26.1.1.0, 32 Mbps of guaranteed bandwidth with low loss
- From Site C (defined as all traffic arriving at interface FE2/1): towards subnet 26.1.1.0, 30 Mbps of guaranteed bandwidth with low loss.

Figure 29 Sample Topology for Guaranteed Bandwidth Services (traversing POS interfaces) to a Single Destination Prefix

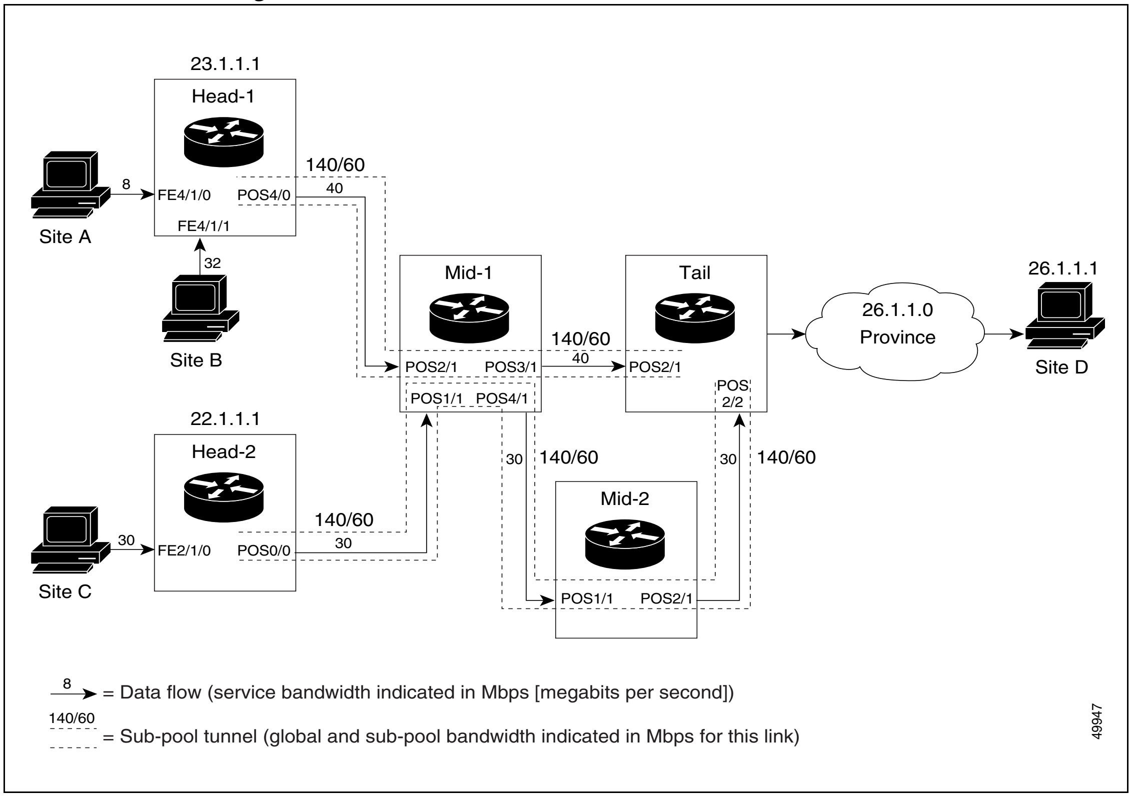


Figure 30 Sample Topology for Guaranteed Bandwidth Services (traversing ATM-PVC interfaces) to a Single Destination Prefix

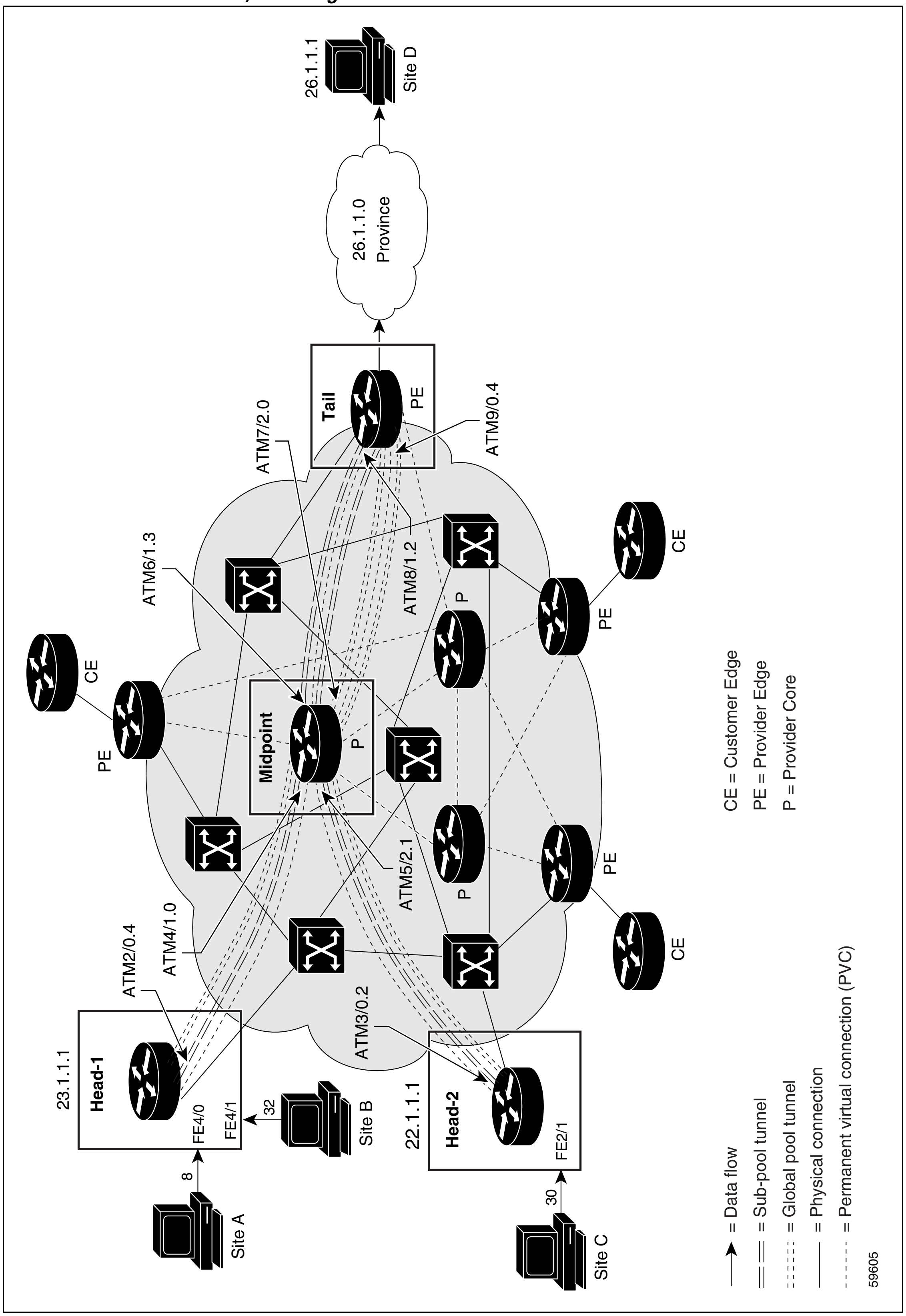
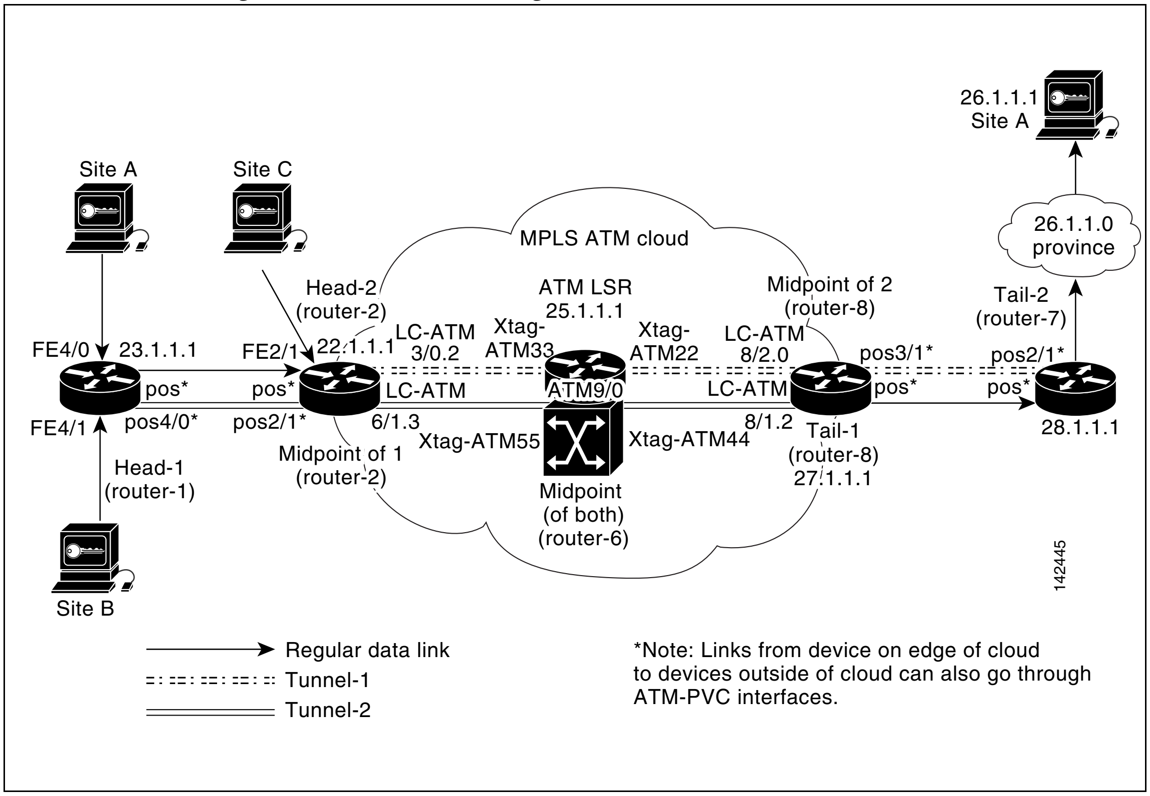


Figure 31 Sample Topology for Guaranteed Bandwidth Services (traversing LC-ATM and XTag-ATM interfaces) to a Single Destination Prefix



These three services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the router-4 tail (in our LC-ATM example, to tail router-8)
- From the Head-2 router, 22.1.1.1, to the router-4 tail (in our LC-ATM example, to tail router-7)

In the POS and ATM-PVC examples, both tunnels use the same tail router, though they have different heads. This is to illustrate that many combinations are possible. (In Figure 5 one midpoint router is shared by both tunnels. In the real world there could of course be many more midpoints.)

All POS, ATM-PVC, LC-ATM, and XTagATM interfaces in this example are OC3, whose capacity is 155 Mbps.

Configuring Tunnel Head-1

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier on page 14). Then we present the QoS commands that guarantee end-to-end service on the subpool tunnel. With the 7200 router, Modular QoS CLI is used.

Configuring the Pools and Tunnel

At the device level:

```
router-1(config)# ip cef
router-1(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# **router isis**	**router ospf 100**
router-1(config-router)# **net 49.0000.1000.0000.0010.00**	**redistribute connected**
router-1(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-1(config-router)# **is-type level-1**	**network 23.1.1.1 0.0.0.0 area 0**
router-1(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**
router-1(config-router)# **passive-interface Loopback0**	

[now one resumes the common command set]:

```
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
```

Create a virtual interface:

```
router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-1(config)# **interface atm2/0**	**interface POS4/0**

[then continue each case at the network interface level:

router-1(config-if)# **mpls traffic-eng tunnels**	**ip address 10.1.1.1 255.255.255.0**
router-1(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-1(config-if)# **interface atm2/0.4**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-1(config-subif)# **ip address 10.1.1.1 255.255.255.0**	
router-1(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-1(config-subif)# **mpls traffic-eng tunnels**	
router-1(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-1(config-subif)# **ip router isis**	
router-1(config-subif)# **exit**	
router-1(config-if)#	[If using IS-IS instead of OSPF]: **ip router isis**

Continuing at the network interface level, regardless of interface type:

```
router-1(config-if)# exit
```

At the tunnel interface:

```
router-1(config)# interface Tunnel1
router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
```

To ensure that packets destined to host 26.1.1.1 and subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```
router-1(config)# ip route 26.1.1.0 255.255.255.0 Tunnel1
router-1(config)# exit
```

And in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```
router-1(config)# no tunnel mpls traffic-eng autoroute announce
```

For Service from Site A to Site D

At the inbound network interface (FE4/0):

1. In global configuration mode, create a class of traffic matching ACL 100, called "sla-1-class":

```
class-map match-all sla-1-class
    match access-group 100
```

2. Create an ACL 100 to refer to all packets destined to 26.1.1.1:

```
access-list 100 permit ip any host 26.1.1.1
```

3. Create a policy named “sla-1-input-policy”, and according to that policy:
   a. Packets in the class called “sla-1-class” are rate-limited to:
      – a rate of 8 million bits per second
      – a normal burst of 1 million bytes
      – a maximum burst of 2 million bytes
   b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.
   c. Packets which exceed this rate are dropped.
   d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-1-input-policy
  class sla-1-class
   police 8000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
           exceed-action drop
  class class-default
   set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE4/0.

```
interface FastEthernet4/0
    service-policy input sla-1-input-policy
```

For Service from Site B to Subnet “Province”

At the inbound network interface (FE4/1):

1. In global configuration mode, create a class of traffic matching ACL 120, called "sla-2-class":

```
class-map match-all sla-2-class
    match access-group 120
```

2. Create an ACL, 120, to refer to all packets destined to subnet 26.1.1.0:

```
access-list 120 permit ip any 26.1.1.0 0.0.0.255
```

3. Create a policy named “sla-2-input-policy”, and according to that policy:
   a. Packets in the class called “sla-2-class” are rate-limited to:
      – a rate of 32 million bits per second
      – a normal burst of 1 million bytes

- a maximum burst of 2 million bytes

b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

c. Packets which exceed this rate are dropped.

d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-2-input-policy
  class sla-2-class
   police 32000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
          exceed-action drop
  class class-default
   set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE4/1.

```
interface FastEthernet4/1
   service-policy input sla-2-input-policy
```

For Both Services

The outbound interface (POS4/0 in Figure 5 and Figure 7, and ATM2/0.4 in Figure 6) is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```
class-map match-all exp-5-traffic
   match mpls experimental 5
```

2. Create a policy named “output-interface-policy”. According to that policy, packets in the class “exp-5-traffic” are put in the priority queue (which is rate-limited to 62 kbits/sec).

```
policy-map output-interface-policy
   class exp-5-traffic
      priority 62
```

3. The policy is applied to packets exiting subinterface ATM2/0.4 (left column, below) or interface POS4/0 (right column):

interface atm2/0 interface atm2/0.4 service-policy output output-interface-policy	interface POS4/0 service-policy output\ output-interface-policy

The result of the above configuration lines is that packets entering the router via interface FE4/0 destined to host 26.1.1.1, or entering the router via interface FE4/1 destined to subnet 26.1.1.0, will have their MPLS experimental bit set to 5. We assume that no other packets entering the router (on any interface) are using this value. (If this cannot be assumed, an additional configuration must be added to mark all such packets to another experimental value.) Packets marked with experimental bit 5, when exiting the router via interface POS4/0 or subinterface ATM2/0.4, will be placed into the priority queue.

Configuring Tunnel Head-2

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier on page 16). Then we present the QoS commands that guarantee end-to-end service on the subpool tunnel. With the 7200 router, Modular QoS CLI is used. [And because this router is on the edge of the MPLS ATM cloud in Figure 7, an LC-ATM interface is configured in that example.]

Configuring the Pools and Tunnel

At the device level:

```
router-2(config)# ip cef
router-2(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

`router-2(config)# router isis`	`router ospf 100`
`router-2(config-router)# net 49.0000.1000.0000.0011.00`	`redistribute connected`
`router-2(config-router)# metric-style wide`	`network 11.1.1.0 0.0.0.255 area 0`
`router-2(config-router)# is-type level-1`	`network 22.1.1.1 0.0.0.0 area 0`
`router-2(config-router)# mpls traffic-eng level-1`	`mpls traffic-eng area 0`
`router-2(config-router)# passive-interface Loopback0`	

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# no ip directed-broadcast
router-2(config-if)# exit
```

For the outgoing network interface:

[ATM cases appear on the left; POS case on the right]:

`router-2(config)# interface atm3/0`	`interface POS0/0`

[then continue each case at the network interface level]:

`router-2(config-if)# mpls traffic-eng tunnels`	`ip address 11.1.1.1 255.0.0.0`
`router-2(config-if)# ip rsvp bandwidth 140000 140000\ sub-pool 60000`	`mpls traffic-eng tunnels`
`router-2(config-if)# interface atm3/0.2` [append the keyword `mpls` if LC-ATM]	`ip rsvp bandwidth 140000 140000\ sub-pool 60000`
`router-2(config-subif)# ip address 11.1.1.1 255.0.0.0`	
`router-2(config-subif)#ip rsvp bandwidth 140000 140000 sub-pool 60000`	
`router-2(config-subif)# mpls traffic-eng tunnels`	
`router-2(config-subif)#` [if ATM-PVC] : `atm pvc 10 10 100 aal5snap` [if LC-ATM] : `mpls atm vpi 2-5`	
[if using IS-IS instead of OSPF]:	
`router-2(config-subif)# ip router isis`	
`router-2(config-subif)# exit`	
`router-2(config-if)#`	[If using IS-IS instead of OSPF]: `ip router isis`

Continuing at the network interface level, regardless of interface type:

```
router-2(config-if)# exit
```

At the tunnel interface:

```
router-2(config)# interface Tunnel2
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
    [though in Figure 7: tunnel destination 28.1.1.1 ]
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
```

To ensure that packets destined to subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```
router-2(config)# ip route 26.1.1.0 255.255.255.0 Tunnel2
router-2(config)# exit
```

And in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```
router-2(config)# no tunnel mpls traffic-eng autoroute announce
```

For Service from Site C to Subnet "Province"

At the inbound network interface (FE2/1):

1. In global configuration mode, create a class of traffic matching ACL 130, called "sla-3-class":

```
class-map match-all sla-3-class
    match access-group 130
```

2. Create an ACL, 130, to refer to all packets destined to subnet 26.1.1.0:

```
access-list 130 permit ip any 26.1.1.0 0.0.0.255
```

3. Create a policy named "sla-3-input-policy", and according to that policy:
    a. Packets in the class called "sla-3-class" are rate-limited to:
        – a rate of 30 million bits per second
        – a normal burst of 1 million bytes
        – a maximum burst of 2 million bytes
    b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.
    c. Packets which exceed this rate are dropped.
    d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-3-input-policy
  class sla-3-class
    police 30000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
           exceed-action drop
  class class-default
    set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE2/1.

```
interface FastEthernet2/1
    service-policy input sla-3-input-policy
```

The outbound interface (POS0/0 or ATM3/0.2) is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```
class-map match-all exp-5-traffic
   match mpls experimental 5
```

2. Create a policy named “output-interface-policy”. According to that policy, packets in the class “exp-5-traffic” are put in the priority queue (which is rate-limited to 32 kbits/sec).

```
policy-map output-interface-policy
   class exp-5-traffic
      priority 32
```

3. The policy is applied to packets exiting interface ATM3/0.2 (left column, below) or POS0/0 (right column):

`interface atm3/0`	`interface POS0/0`
`interface atm3/0.2`	`service-policy output\ output-interface-policy`
`service-policy output output-interface-policy`	

The result of the above configuration lines is that packets entering the router via interface FE2/1 destined to subnet 26.1.1.0, will have their MPLS experimental bit set to 5. We assume that no other packets entering the router (on any interface) are using this value. (If this cannot be assumed, an additional configuration must be added to mark all such packets to another experimental value.) Packets marked with experimental bit 5, when exiting the router via interface POS0/0 or ATM3/0.2, will be placed into the priority queue.

Tunnel Midpoint Configurations

All four interfaces on the 7200 midpoint router (“**Mid-1**” in Figure 5, “**Midpoint**” in Figure 6) are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces).

When an ATM-LSR serves as a midpoint (as in Figure 7), its XTagATM interfaces and BPX or IGX switching resources must be configured. Also, two new MPLS commands are used. The details of this configuration are presented in the ATM-LSR section which begins on page 38.

The LC-ATM midpoint configuration (on the left edge of the ATM cloud in Figure 7) is presented on page 35. LC-ATM at a midpoint on the right edge of the cloud in Figure 7 is presented on page 39.

Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

`router-3(config)# router isis`	`router ospf 100`
`router-3(config-router)# net 49.0000.2400.0000.0011.00`	`redistribute connected`
`router-3(config-router)# metric-style wide`	`network 10.1.1.0 0.0.0.255 area 0`
`router-3(config-router)# is-type level-1`	`network 11.1.1.0 0.0.0.255 area 0`
`router-3(config-router)# mpls traffic-eng level-1`	`network 24.1.1.1 0.0.0.0 area 0`
`router-3(config-router)# passive-interface Loopback0`	`network 12.1.1.0 0.0.0.255 area 0`
`router-3(config-router)#`	`network 13.1.1.0 0.0.0.255 area 0`
`router-3(config-router)#`	`mpls traffic-eng area 0`

[now one resumes the common command set]:

```
router-3(config-router)# mpls traffic-eng router-id Loopback0
```

```
router-3(config-router)# exit
```

Create a virtual interface:

```
router-3(config)# interface Loopback0
router-3(config-if)# ip address 22.1.1.1 255.255.255.255
router-3(config-if)# exit
```

For one incoming network interface, first at the device level:

[ATM-PVC case appears on the left; POS case on the right]:

```
router-3(config)# interface atm4/1                    | interface POS2/1
```

[then continue each case at the network interface level]:

```
router-3(config-if)# mpls traffic-eng tunnels         | ip address 10.1.1.2 255.0.0.0
router-3(config-if)# ip rsvp bandwidth 140000 140000\ | mpls traffic-eng tunnels
                     sub-pool 60000                   |
router-3(config-if)# interface atm4/1.0               | ip rsvp bandwidth 140000 140000\
                                                      |    sub-pool 60000
router-3(config-subif)# ip address 10.1.1.2 255.0.0.0 |
router-3(config-subif)#ip rsvp bandwidth 140000 140000|
                     sub-pool 60000                   |
router-3(config-subif)# mpls traffic-eng tunnels      |
router-3(config-subif)# atm pvc 10 10 100 aal5snap    |
[if using IS-IS instead of OSPF]:                     |
router-3(config-subif)# ip router isis                |
router-3(config-subif)# exit                          |
router-3(config-if)#                                  | [If using IS-IS instead of OSPF]:
                                                      | ip router isis
```

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

For the other incoming network interface, first at the device level:

[ATM-PVC case appears on the left; POS case on the right]:

```
router-3(config)# interface atm5/2                    | interface POS1/1
```

[then continuing each case at the network interface level]:

```
router-3(config-if)# mpls traffic-eng tunnels         | ip address 11.1.1.2 255.0.0.0
router-3(config-if)# ip rsvp bandwidth 140000 140000/ | mpls traffic-eng tunnels
                     sub-pool 60000                   |
router-3(config-if)# interface atm5/2.1               | ip rsvp bandwidth 140000 140000/
                                                      |    sub-pool 60000
router-3(config-subif)# ip address 11.1.1.2 255.0.0.0 |
router-3(config-subif)#ip rsvp bandwidth 140000 140000\|
                     sub-pool 60000                   |
router-3(config-subif)# mpls traffic-eng tunnels      |
router-3(config-subif)# atm pvc 10 10 100 aal5snap    |
[if using IS-IS instead of OSPF]:                     |
router-3(config-subif)# ip router isis                |
router-3(config-subif)# exit                          |
router-3(config-if)#                                  | [If using IS-IS instead of OSPF]:
                                                      | ip router isis
```

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

For one outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

ATM-PVC case:

```
router-3(config)# interface atm6/1
```

[then continue each case at the network interface level]:

```
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000\
                     sub-pool 60000
router-3(config-if)# interface atm6/1.3

router-3(config-subif)# ip address 11.1.1.2 255.0.0.0
router-3(config-subif)#ip rsvp bandwidth 140000 140000\
                     sub-pool 60000
router-3(config-subif)# mpls traffic-eng tunnels
router-3(config-subif)# atm pvc 10 10 100 aal5snap
```

[if using IS-IS instead of OSPF]:

```
router-3(config-subif)# ip router isis
router-3(config-subif)# exit
router-3(config-if)#
```

POS case:

```
interface POS3/1
ip address 11.1.1.2 255.0.0.0
mpls traffic-eng tunnels
ip rsvp bandwidth 140000 140000\
   sub-pool 60000
```

[If using IS-IS instead of OSPF]:

```
ip router isis
```

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

For the other outgoing network interface, first at the device level:

[ATM-PVC case appears on the left; POS case on the right]:

ATM-PVC case:

```
router-3(config)# interface atm7/2
```

[then, continuing each case at the network interface level]:

```
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000\
                     sub-pool 60000
router-3(config-if)# interface atm7/2.0

router-3(config-subif)# ip address 12.1.1.1 255.0.0.0
router-3(config-subif)#ip rsvp bandwidth 140000 140000\
                     sub-pool 60000
router-3(config-subif)# mpls traffic-eng tunnels
router-3(config-subif)# atm pvc 10 10 100 aal5snap
```

[if using IS-IS instead of OSPF]:

```
router-3(config-subif)# ip router isis
router-3(config-subif)# exit
router-3(config-if)#
```

POS case:

```
interface POS3/1
ip address 12.1.1.1 255.0.0.0
mpls traffic-eng tunnels
ip rsvp bandwidth 140000 140000\
   sub-pool 60000
```

[If using IS-IS instead of OSPF]:

```
ip router isis
```

Continuing at the network interface level, regardless of interface type:

```
router-3(config-if)# exit
```

Tunnel Midpoint Configuration [Midpoint-1 in Figure 7, POS ingress, LC-ATM egress]

Configuring the Pools and Tunnels

At the device level:

```
router-2(config)# ip cef
router-2(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# **router isis**	**router ospf 100**
router-2(config-router)# **net 49.0000.2400.0000.0011.00**	**redistribute connected**
router-2(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-2(config-router)# **is-type level-1**	**network 11.1.1.0 0.0.0.255 area 0**
router-2(config-router)# **mpls traffic-eng level-1**	**network 24.1.1.1 0.0.0.0 area 0**
router-2(config-router)# **passive-interface Loopback0**	**network 12.1.1.0 0.0.0.255 area 0**
router-2(config-router)#	**network 13.1.1.0 0.0.0.255 area 0**
router-2(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# exit
```

For the incoming network interface, first at the device level:

```
router-2(config)# interface POS2/1
```

[then continuing at the network interface level]:

```
router-2(config-if)# ip address 11.1.1.2 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
```

[If using IS-IS instead of OSPF]:

```
router-2(config-if)# ip router isis
```

[and in both cases]:

```
router-2(config-if)# exit
```

For the outgoing network interface:

```
router-2(config)# interface atm6/1
 router-2(config-if)# mpls traffic-eng tunnels
 router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
 router-2(config-if)# interface atm6/1.3 mpls
  router-2(config-subif)# ip address 11.1.1.2 255.0.0.0
  router-2(config-subif)#ip rsvp bandwidth 140000 140000 sub-pool 60000
  router-2(config-subif)# mpls traffic-eng tunnels
  router-2(config-subif)# mpls atm vpi 2-15
```

[if using IS-IS instead of OSPF]:

```
  router-2(config-subif)# ip router isis
  router-2(config-subif)# exit
```

[and in bothcases]:

```
 router-2(config-if)# exit
```

Tunnel Midpoint Configuration [Mid-2 in Figure 5, all POS]

[For the sake of simplicity, the ATM-PVC example (Figure 6) was illustrated with only one midpoint router.]

Both interfaces on the second 7200 midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

Configuring the Pools and Tunnel

At the device level:

```
router-5(config)# ip cef
router-5(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-5(config)# **router isis**	**router ospf 100**
router-5(config-router)# **net 49.2500.1000.0000.0012.00**	**redistribute connected**
router-5(config-router)# **metric-style wide**	**network 13.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **is-type level-1**	**network 14.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **mpls traffic-eng level-1**	**network 25.1.1.1 0.0.0.0 area 0**
router-5(config-router)# **passive-interface Loopback0**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit
```

Create a virtual interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit
```

At the incoming network interface level:

```
router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
```

[and if using IS-IS instead of OSPF]:

```
router-5(config-if)# ip router isis
```

[and in all cases]:

```
router-5(config-if)# exit
```

At the outgoing network interface level:

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
```

[and if using IS-IS instead of OSPF]:

```
router-5(config-if)# ip router isis
```

[and in all cases]:

```
router-5(config-if)# exit
```

Tunnel Midpoint Configuration [ATM-LSR in Figure 7, all XTag-ATM]

When an ATM-LSR serves as a midpoint, its Virtual Switch Interface, XTagATM interfaces, and BPX or IGX switching resources must be configured. Also, one or two new MPLS commands are used on the ATM-LSR (namely, **mpls traffic-eng atm cos sub-pool** and **mpls traffic-eng atm cos global-pool**), to transfer traffic from priority queues into class-of-service (since the cell-based switch cannot examine packets).

Configuring the Pools and Tunnel

At the device level:

```
router-6(config)# ip cef
router-6(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

```
router-6(config)# router isis                                    | router ospf 100
 router-6(config-router)# net 49.0000.2400.0000.0011.00          | redistribute connected
 router-6(config-router)# metric-style wide                      | network 10.1.1.0 0.0.0.255 area 0
 router-6(config-router)# is-type level-1                        | network 11.1.1.0 0.0.0.255 area 0
 router-6(config-router)# mpls traffic-eng level-1               | network 24.1.1.1 0.0.0.0 area 0
 router-6(config-router)# passive-interface Loopback0            | network 12.1.1.0 0.0.0.255 area 0
 router-6(config-router)#                                        | network 13.1.1.0 0.0.0.255 area 0
 router-6(config-router)#                                        | mpls traffic-eng area 0
```

[now one resumes the common command set]:

```
router-6(config-router)# mpls traffic-eng router-id Loopback0
router-6(config-router)# exit
```

Create a virtual interface:

```
router-6(config)# interface Loopback0
router-6(config-if)# ip address 25.1.1.1 255.255.255.255
router-6(config-if)# exit
```

At the device level, to coordinate traffic across the router and switch portions of the device:

```
router-6(config)# interface atm9/0 0/0/0
router-6(config-if)# label-control-protocol vsi
router-6(config-if)# exit
router-6(config)# mpls traffic-eng atm cos sub-pool
router-6(config)# mpls traffic-eng atm cos global-pool premiun
```

For one incoming network interface:

```
router-6(config)# interface Xtagatm22
    router-6(config-if)# extended-port atm9/0 bpx2.2
    router-6(config-if)# ip address 10.1.1.2 255.0.0.0
    router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
    router-6(config-if)# mpls traffic-eng tunnels
    router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
```

[and in either case]:

```
router-6(config-if)# exit
```

For the other incoming network interface:

```
router-6(config)# interface xtagatm55
    router-6(config-if)# extended-port atm9/0 bpx5.5
    router-6(config-if)# ip address 11.1.1.2 255.0.0.0
    router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
    router-6(config-if)# mpls traffic-eng tunnels
    router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
```

[and in either case]:

```
router-6(config-if)# exit
```

For one outgoing network interface:

```
router-6(config)# interface Xtagatm33
    router-6(config-if)# extended-port atm9/0 bpx3.3
    router-6(config-if)# ip address 11.1.1.2 255.0.0.0
    router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
    router-6(config-if)# mpls traffic-eng tunnels
    router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
```

[and in either case]:

```
router-6(config-if)# exit
```

For the other outgoing network interface:

```
router-6(config)# interface Xtagatm44
    router-6(config-if)# extended-port atm9/0 bpx4.4
    router-6(config-if)# ip address 12.1.1.1 255.0.0.0
    router-6(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
    router-6(config-if)# mpls traffic-eng tunnels
    router-6(config-if)# mpls atm vpi 2-15
```

[If using IS-IS instead of OSPF]:

```
router-6(config-if)# ip router isis
```

[and in either case]:

```
router-6(config-if)# exit
```

Tunnel Midpoint Configuration [Figure 7: Midpoint of Tunnel 2, LC-ATM Ingress]

This 7200 midpoint router sits at the right-side edge of the MPLS ATM cloud in Figure 7. Therefore its ingress interface is LC-ATM and its egress can be either POS or ACM-PVC.

Configuring the Pools and Tunnels

At the device level:

```
router-8(config)# ip cef
router-8(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

```
router-8(config)# router isis                            | router ospf 100
 router-8(config-router)# net 49.2500.1000.0000.0012.00  | redistribute connected
 router-8(config-router)# metric-style wide              | network 13.1.1.0 0.0.0.255 area 0
 router-8(config-router)# is-type level-1                | network 14.1.1.0 0.0.0.255 area 0
 router-8(config-router)# mpls traffic-eng level-1       | network 25.1.1.1 0.0.0.0 area 0
 router-8(config-router)# passive-interface Loopback0    | mpls traffic-eng area 0
```

[now one resumes the common command set]:

```
router-8(config-router)# mpls traffic-eng router-id Loopback0
router-8(config-router)# exit
```

Create a virtual interface:

```
router-8(config)# interface Loopback0
router-8(config-if)# ip address 27.1.1.1 255.255.255.255
router-8(config-if)# exit
```

At the incoming network interface level:

```
router-8(config)# interface atm8/2
    router-8(config-if)# mpls traffic-eng tunnels
    router-8(config-if)# ip rsvp bandwidth 140000 140000\ sub-pool 60000
    router-8(config-if)# interface atm8/2.0 mpls
    router-8(config-subif)# ip address 13.1.1.2 255.0.0.0
    router-8(config-subif)# ip rsvp bandwidth 140000 140000 sub-pool 60000
    router-8(config-subif)# mpls traffic-eng tunnels
    router-8(config-subif)# mpls atm vpi 2-15
```

[if using IS-IS instead of OSPF]:

```
router-8(config-subif)# ip router isis
router-8(config-subif)# exit
```

And in all cases:

```
router-8(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

`router-8(config)# interface atm6/1`	`interface POS3/1`
[then continue each case at the network interface level]:	
`router-8(config-if)# mpls traffic-eng tunnels`	`ip address 14.1.1.1 255.0.0.0`
`router-8(config-if)# ip rsvp bandwidth 140000 140000\ sub-pool 60000`	`mpls traffic-eng tunnels`
`router-8(config-if)# interface atm6/1.3`	`ip rsvp bandwidth 140000 140000\ sub-pool 60000`
`router-8(config-subif)# ip address 14.1.1.1 255.0.0.0`	
`router-8(config-subif)#ip rsvp bandwidth 140000 140000\ sub-pool 60000`	
`router-8(config-subif)# mpls traffic-eng tunnels`	
`router-8(config-subif)# atm pvc 10 10 100 aal5snap`	
[if using IS-IS instead of OSPF]:	
`router-8(config-subif)# ip router isis`	
`router-8(config-subif)# exit`	
`router-8(config-if)#`	[If using IS-IS instead of OSPF]: `ip router isis`

Continuing at the network interface level, regardless of interface type:

```
router-8(config-if)# exit
```

Tunnel Tail Configuration

The inbound interfaces on the 7200 tail router are configured identically to the inbound interfaces of the midpoint routers (except, of course, for the ID of each particular interface):

Configuring the Pools and Tunnels

At the device level:

```
router-4-8-or-7(config)# ip cef
router-4-8-or-7(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

`router-4-8-or-7(config)# router isis`	`router ospf 100`
`router-4-8-or-7(config-router)# net 49.0000.2700.0000.0000.00`	`redistribute connected`
`router-4-8-or-7(config-router)# metric-style wide`	`network 12.1.1.0 0.0.0.255 area 0`
`router-4-8-or-7(config-router)# is-type level-1`	`network 14.1.1.0 0.0.0.255 area 0`
`router-4-8-or-7(config-router)# mpls traffic-eng level-1`	`network 27.1.1.1 0.0.0.0 area 0`
`router-4-8-or-7(config-router)# passive-interface Loopback0`	`mpls traffic-eng area 0`

[now one resumes the common command set]:

```
router-4-8-or-7(config-router)# mpls traffic-eng router-id Loopback0
router-4-8-or-7(config-router)# exit
```

Create a virtual interface:

```
router-4-8-or-7(config)# interface Loopback0
router-4-8-or-7(config-if)# ip address 27.1.1.1 255.255.255.255
[but on router-7 in Figure 7 use ip address 28.1.1.1 255.255.255.255 ]
router-4-8-or-7(config-if)# exit
```

For the incoming network interface, first at the device level:

[LC-ATM case appears on the left; POS case on the right]:

LC-ATM	POS
`router-4-8-or-7(config)# interface atm8/1`	`interface POS2/1`

[then continue each case at the network interface level]:

LC-ATM	POS
`router-4-8-or-7(config-if)# mpls traffic-eng tunnels`	`ip address 12.1.1.2 255.0.0.0`
`router-4-8-or-7(config-if)# ip rsvp bandwidth 140000\ 140000 sub-pool 60000`	`mpls traffic-eng tunnels`
`router-4-8-or-7(config-if)# interface atm8/1.2 mpls`	`ip rsvp bandwidth 140000 140000\ sub-pool 60000`
`router-4-8-or-7(config-subif)# ip address 12.1.1.2 255.0.0.0`	
`router-4-8-or-7(config-subif)#ip rsvp bandwidth 140000\ 140000 sub-pool 60000`	
`router-4-8-or-7(config-subif)# mpls traffic-eng tunnels`	
`router-4-8-or-7(config-subif)# mpls atm vpi 2-5`	
[if using IS-IS instead of OSPF]:	
`router-4-8-or-7(config-subif)# ip router isis`	
`router-4-8-or-7(config-subif)# exit`	
`router-4-8-or-7(config-if)#`	[If using IS-IS instead of OSPF]: `ip router isis`

Continuing at the network interface level, regardless of interface type:

```
router-4-8-or-7(config-if)# exit
```

Because the tunnel ends on the tail (does not include any outbound interfaces of the tail router), no outbound QoS configuration is used.

Example with Many Destination Prefixes

Figure 8 and Figure 9 illustrate topologies for guaranteed bandwidth services whose destinations are a set of prefixes. In Figure 8 the interfaces to be configured are POS (Packet over SONET), while in Figure 9 the interfaces are ATM-PVC (Asynchronous Transfer Mode – Permanent Virtual Circuit). In both illustrations, the destinations' prefixes usually share some common properties such as belonging to the same Autonomous System (AS) or transiting through the same AS. Although the individual prefixes may change dynamically because of route flaps in the downstream autonomous systems, the properties the prefixes share will not change. Policies addressing the destination prefix set are enforced through Border Gateway Protocol (BGP), which is described in the following documents:

- "Configuring QoS Policy Propagation via Border Gateway Protocol" in the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.1 (http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt1/qcdprop.htm)
- "Configuring BGP" in the *Cisco IOS IP and IP Routing Configuration Guide,* Release 12.1 (http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdbgp.htm)

- "BGP Commands" in the *Cisco IOS IP and IP Routing Command Reference,* Release 12.1 (http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/1rdbgp.htm)

In this example, three guaranteed bandwidth services are offered:

- Traffic coming from Site A (defined as all traffic arriving at interface FE4/0) and from Site C (defined as all traffic arriving at interface FE2/1) destined to AS5
- Traffic coming from Sites A and C that transits AS5 but is not destined to AS5. (In the figure, the transiting traffic will go to AS6 and AS7)
- Traffic coming from Sites A and C destined to prefixes advertised with a particular BGP community attribute (100:1). In this example, Autonomous Systems #3, #5, and #8 are the BGP community assigned the attribute 100:1.

Figure 32 Sample Topology for Guaranteed Bandwidth Service (traversing POS interfaces) to Many Destination Prefixes

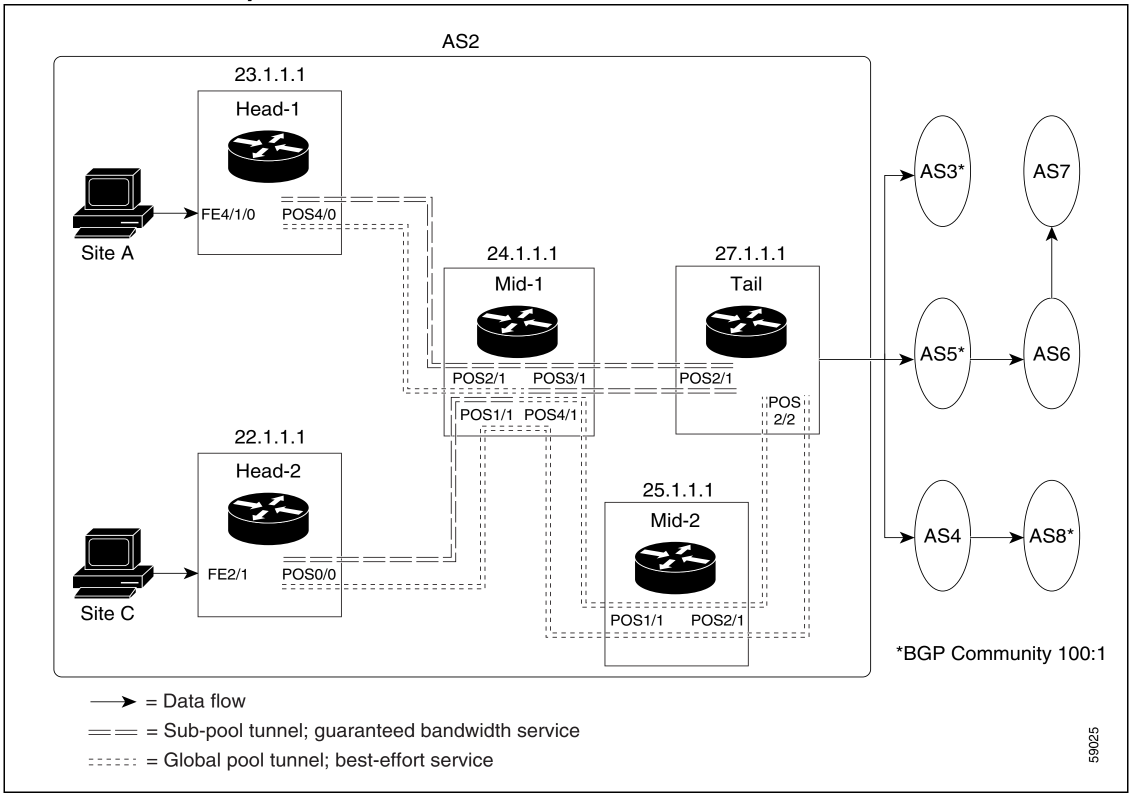
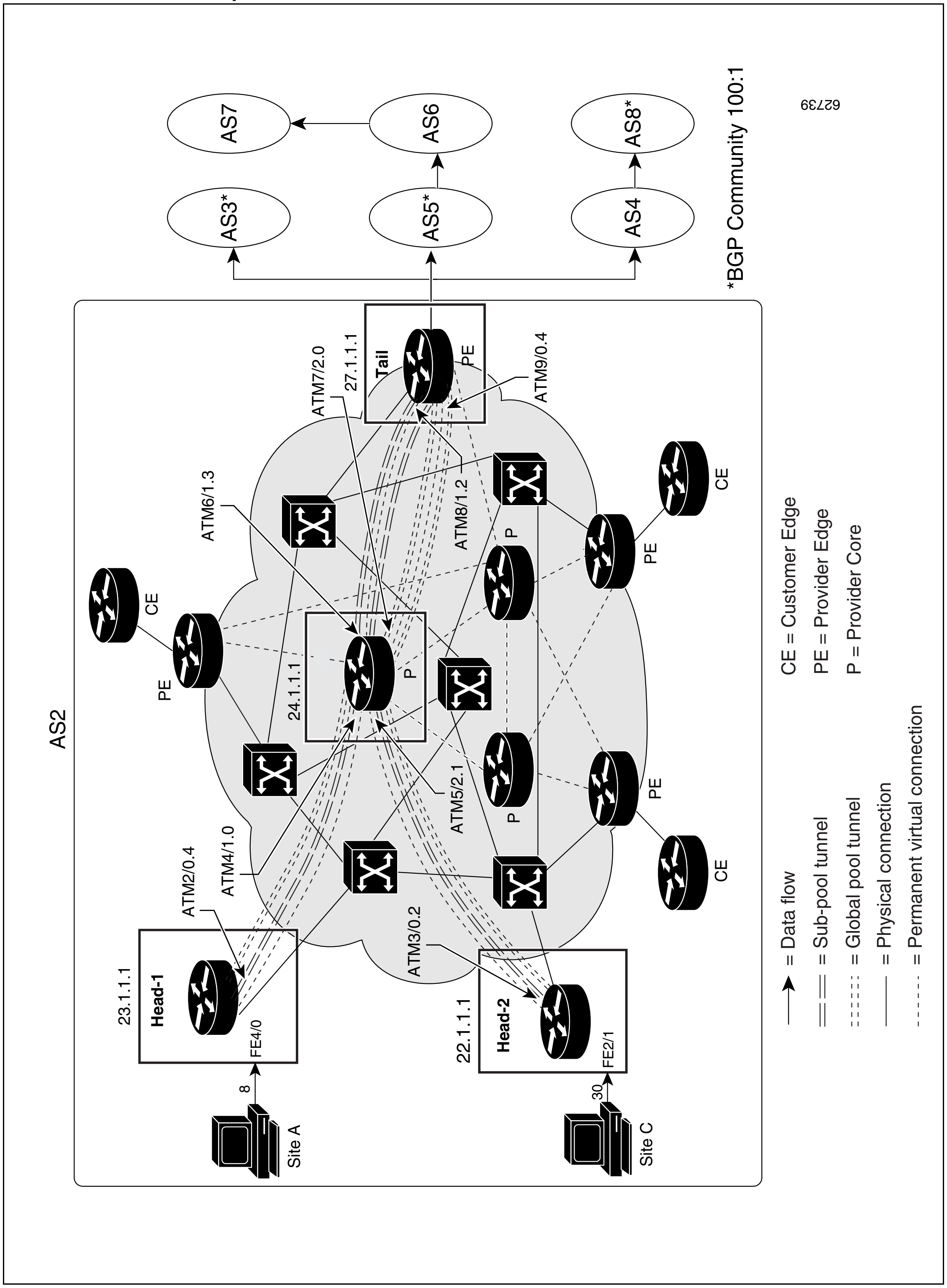


Figure 33 Sample Topology for Guaranteed Bandwidth Service (traversing ATM-PVC interfaces) to Many Destination Prefixes



The applicability of guaranteed bandwidth service is not limited to the three types of multiple destination scenarios described above. There is not room in this document to present all possible scenarios. These three were chosen as representative of the wide range of possible deployments.

The guaranteed bandwidth services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the tail
- From the Head-2 router, 22.1.1.1, to that same tail

In addition, a global pool tunnel has been configured from each head end, to carry best-effort traffic to the same destinations. All four tunnels use the same tail router, even though they have different heads and differ in their passage through the midpoint(s). (Of course in the real world there would likely be many more midpoints than just the one or two shown here.)

All POS and ATM-PVC interfaces in this example are OC3, whose capacity is 155 Mbps.

Configuring a multi-destination guaranteed bandwidth service involves:

a. Building a sub-pool MPLS-TE tunnel
b. Configuring DiffServ QoS
c. Configuring QoS Policy Propagation via BGP (QPPB)
d. Mapping traffic onto the tunnels

All of these tasks are included in the following example.

Tunnel Head Configuration [Head-1]

First we recapitulate commands that establish a sub-pool tunnel (commands presented earlier on page 9) and now we also configure a global pool tunnel. Additionally, we present QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (With the 7200 router, Modular QoS CLI is used).

Configuring the Pools and Tunnels

At the device level:

```
router-1(config)# ip cef
router-1(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

`router-1(config)# router isis`	`router ospf 100`
`router-1(config-router)# net 49.0000.1000.0000.0010.00`	`redistribute connected`
`router-1(config-router)# metric-style wide`	`network 10.1.1.0 0.0.0.255 area 0`
`router-1(config-router)# is-type level-1`	`network 23.1.1.1 0.0.0.0 area 0`
`router-1(config-router)# mpls traffic-eng level-1`	`mpls traffic-eng area 0`

[now one resumes the common command set]:

```
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
```

Create a virtual interface:

```
router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

`router-1(config)# interface atm2/0`	`interface POS4/0`

[then continue each case at the network interface level:

```
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 140000 140000\
                    sub-pool 60000
router-1(config-if)# interface atm2/0.4

router-1(config-subif)# ip address 10.1.1.1 0.0.0.0
router-1(config-subif)#ip rsvp bandwidth 140000 140000\
                    sub-pool 60000
router-1(config-subif)# mpls traffic-eng tunnels
router-1(config-subif)# atm pvc 10 10 100 aal5snap
```

[if using IS-IS instead of OSPF]:

```
router-1(config-subif)# ip router isis
router-1(config-subif)# exit
```

```
ip address 10.1.1.1 255.0.0.0
mpls traffic-eng tunnels

ip rsvp bandwidth 140000 140000\
   sub-pool 60000
```

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-1(config-if)# ip router isis
```

[and in all cases]:

```
router-1(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-1(config)# interface Tunnel1
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path1
router-1(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-1(config)# interface Tunnel2
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth 80000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
   best-effort-path1
router-1(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-1(config)# ip explicit-path name gbs-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
router-1(config)# ip explicit-path name best-effort-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 25.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

Configuring DiffServ QoS

At the inbound network interface (in Figure 8 and Figure 9 this is FE4/0), packets received are rate-limited to:

a. a rate of 30 Mbps
b. a normal burst of 1 MB
c. a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```
router-1(config)# interface FastEthernet4/0
router-1(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
   conform-action set-mpls-exp-transmit 5 exceed-action drop
router-1(config-if)# bgp-policy destination ip-qos-map
router-1(config-if)# exit
```

At the device level create a class of traffic called "exp5-class" that has MPLS experimental bit set to 5:

```
router-1(config)# class-map match-all exp5-class
router-1(config-cmap)# match mpls experimental 5
router-1(config-cmap)# exit
```

Create a policy that creates a priority queue for "exp5-class":

```
router-1(config)# policy-map core-out-policy
router-1(config-pmap)# class exp5-class
router-1(config-pmap-c)# priority 100000
router-1(config-pmap-c)# exit
router-1(config-pmap)# class class-default
router-1(config-pmap-c)# bandwidth 55000
router-1(config-pmap-c)# exit
router-1(config-pmap)# exit
```

The policy is applied to packets exiting subinterface ATM2/0.4 (left side) or interface POS4/0 (right side):

`interface atm2/0` `    interface atm2/0.4` `    service-policy output core-out-policy`	`interface POS4/0` `    service-policy output\` `      core-out-policy`

Configuring QoS Policy Propagation via BGP

For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-1(config)# router bgp 2
router-1(config-router)# no synchronization
router-1(config-router)# table-map set-qos-group
router-1(config-router)# bgp log-neighbor-changes
router-1(config-router)# neighbor 27.1.1.1 remote-as 2
router-1(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-1(config-router)# no auto-summary
router-1(config-router)# exit
```

For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 (a virtual loopback configured in the tail router; see page 57) so they will be mapped onto Tunnel #1 (the guaranteed bandwidth service tunnel). At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 100
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 100 permit ^5$
```

For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 101
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 101 permit _5_
```

For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match community 20
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip community-list 20 permit 100:1
```

Mapping Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #1:

```
router-1(config)# ip route 29.1.1.1 255.255.255.255 Tunnel1
```

Map all best-effort traffic (traveling toward another virtual loopback interface, 30.1.1.1, configured in the tail router) onto Tunnel #2:

```
router-1(config)# ip route 30.1.1.1 255.255.255.255 Tunnel2
```

Tunnel Head Configuration [Head-2]

As with the Head-1 device and interfaces, the following Head-2 configuration first presents commands that establish a sub-pool tunnel (commands presented earlier on page 9) and then also configures a global pool tunnel. After that it presents QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (Because this is a 7200 router, Modular QoS CLI is used).

Configuring the Pools and Tunnels

At the device level:

```
router-2(config)# ip cef
router-2(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# **router isis**	**router ospf 100**
router-2(config-router)# **net 49.0000.1000.0000.0011.00**	**redistribute connected**
router-2(config-router)# **metric-style wide**	**network 11.1.1.0 0.0.0.255 area 0**
router-2(config-router)# **is-type level-1**	**network 22.1.1.1 0.0.0.0 area 0**
router-2(config-router)# **mpls traffic-eng level-1**	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# exit
```

For the outgoing network interface:

[ATM-PVC case appears on the left; POS case on the right]:

router-2(config)# **interface atm3/0**	**interface POS0/0**

[then continue each case at the network interface level:

router-2(config-if)# **mpls traffic-eng tunnels**	**ip address 11.1.1.1 255.0.0.0**
router-2(config-if)# **ip rsvp bandwidth 140000 140000\ sub-pool 60000**	**mpls traffic-eng tunnels**
router-2(config-if)# **interface atm3/0.2**	**ip rsvp bandwidth 140000 140000\ sub-pool 60000**
router-2(config-subif)# **ip address 11.1.1.1 255.0.0.0**	
router-2(config-subif)#**ip rsvp bandwidth 140000 140000\ sub-pool 60000**	
router-2(config-subif)# **mpls traffic-eng tunnels**	
router-2(config-subif)# **atm pvc 10 10 100 aal5snap**	
[if using IS-IS instead of OSPF]:	
router-2(config-subif)# **ip router isis**	
router-2(config-subif)# **exit**	

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-2(config-if)# ip router isis
```

[and in all cases]:

```
router-2(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-2(config)# interface Tunnel3
router-2(config-if)# ip unnumbered Loopback0
```

```
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path2
router-2(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-2(config)# interface Tunnel4
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth 70000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
   best-effort-path2
router-2(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-2(config)# ip explicit-path name gbs-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
router-2(config)# ip explicit-path name best-effort-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 25.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

Configuring DiffServ QoS

At the inbound network interface (in Figure 8 and Figure 9 this is FE2/1), packets received are rate-limited to:

a. a rate of 30 Mbps

b. a normal burst of 1 MB

c. a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```
router-2(config)# interface FastEthernet2/1
router-2(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
   conform-action set-mpls-exp-transmit 5 exceed-action drop
router-2(config-if)# bgp-policy destination ip-qos-map
router-2(config-if)# exit
```

At the device level create a class of traffic called “exp5-class” that has MPLS experimental bit set to 5:

```
router-2(config)# class-map match-all exp5-class
router-2(config-cmap)# match mpls experimental 5
router-2(config-cmap)# exit
```

Create a policy that creates a priority queue for “exp5-class”:

```
router-2(config)# policy-map core-out-policy
router-2(config-pmap)# class exp5-class
router-2(config-pmap-c)# priority 100000
router-2(config-pmap-c)# exit
router-2(config-pmap)# class class-default
router-2(config-pmap-c)# bandwidth 55000
router-2(config-pmap-c)# exit
router-2(config-pmap)# exit
```

The policy is applied to packets exiting subinterface ATM3/0.2 (left side) or interface POS0/0 (right side):

`interface atm3/0`	`interface POS0/0`
`interface atm3/0.2`	`service-policy output\ core-out-policy`
`service-policy output core-out-policy`	

Configuring QoS Policy Propagation via BGP

For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-2(config)# router bgp 2
router-2(config-router)# no synchronization
router-2(config-router)# table-map set-qos-group
router-2(config-router)# bgp log-neighbor-changes
router-2(config-router)# neighbor 27.1.1.1 remote-as 2
router-2(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-2(config-router)# no auto-summary
router-2(config-router)# exit
```

For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 (a virtual loopback configured in the tail router; see page 57) so they will be mapped onto Tunnel #3 (th e guaranteed bandwidth service tunnel). At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 100
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 100 permit ^5$
```

For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 101
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 101 permit _5_
```

For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match community 20
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip community-list 20 permit 100:1
```

Mapping Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #3:

```
router-2(config)# ip route 29.1.1.1 255.255.255.255 Tunnel3
```

Map all best-effort traffic onto Tunnel #4 (traveling toward another virtual loopback interface, 30.1.1.1, configured in the tail router):

```
router-2(config)# ip route 30.1.1.1 255.255.255.255 Tunnel4
```

Tunnel Midpoint Configuration [Mid-1]

All four interfaces on the midpoint router are configured very much like the outbound interface of the head router. The strategy is to have all mid-point routers in this Autonomous System ready to carry future as well as presently configured sub-pool and global pool tunnels.

Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-3(config)# **router isis**	**router ospf 100**
router-3(config-router)# **net 49.0000.2400.0000.0011.00**	**redistribute connected**
router-3(config-router)# **metric-style wide**	**network 10.1.1.0 0.0.0.255 area 0**
router-3(config-router)# **is-type level-1**	**network 11.1.1.0 0.0.0.255 area 0**
router-3(config-router)# **mpls traffic-eng level-1**	**network 24.1.1.1 0.0.0.0 area 0**
router-3(config-router)#	**network 12.1.1.0 0.0.0.255 area 0**
router-3(config-router)#	**network 13.1.1.0 0.0.0.255 area 0**
router-3(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit
```

Create a virtual interface:

```
router-3(config)# interface Loopback0
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# exit
```

At one incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

`router-3(config)# interface atm4/1`	`interface POS2/1`

[then continue each case at the network interface level:

`router-3(config-if)# mpls traffic-eng tunnels`	`ip address 10.1.1.2 255.0.0.0`
`router-3(config-if)# ip rsvp bandwidth 140000 140000\ sub-pool 70000`	`mpls traffic-eng tunnels`
`router-3(config-if)# interface atm4/1.0`	`ip rsvp bandwidth 140000 140000\ sub-pool 70000`
`router-3(config-subif)# ip address 10.1.1.2 255.0.0.0`	
`router-3(config-subif)#ip rsvp bandwidth 140000 140000\ sub-pool 70000`	
`router-3(config-subif)# mpls traffic-eng tunnels`	
`router-3(config-subif)# atm pvc 10 10 100 aal5snap`	
[if using IS-IS instead of OSPF]:	
`router-3(config-subif)# ip router isis`	
`router-3(config-subif)# exit`	

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
```

[and in all cases]:

```
router-3(config-if)# exit
```

At the other incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

`router-3(config)# interface atm5/2`	`interface POS1/1`

[then continue each case at the network interface level:

`router-3(config-if)# mpls traffic-eng tunnels`	`ip address 11.1.1.2 255.0.0.0`
`router-3(config-if)# ip rsvp bandwidth 140000 140000\ sub-pool 70000`	`mpls traffic-eng tunnels`
`router-3(config-if)# interface atm5/2.1`	`ip rsvp bandwidth 140000 140000\ sub-pool 70000`
`router-3(config-subif)# ip address 11.1.1.2 255.0.0.0`	
`router-3(config-subif)#ip rsvp bandwidth 140000 140000\ sub-pool 70000`	
`router-3(config-subif)# mpls traffic-eng tunnels`	
`router-3(config-subif)# atm pvc 10 10 100 aal5snap`	
[if using IS-IS instead of OSPF]:	
`router-3(config-subif)# ip router isis`	
`router-3(config-subif)# exit`	

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
```

[and in all cases]:

```
router-3(config-if)# exit
```

At the outgoing network interface through which two sub-pool tunnels currently exit:

[ATM-PVC case appears on the left; POS case on the right]:

`router-3(config)# interface atm6/1`	`interface POS3/1`

[then continue each case at the network interface level:

```
router-3(config-if)# mpls traffic-eng tunnels              | ip address 12.1.1.1 255.0.0.0
router-3(config-if)# ip rsvp bandwidth 140000 140000\       | mpls traffic-eng tunnels
                     sub-pool 70000                         |
router-3(config-if)# interface atm6/1.3                    | ip rsvp bandwidth 140000 140000\
                                                            |    sub-pool 70000
router-3(config-subif)# ip address 12.1.1.1 255.0.0.0      |
router-3(config-subif)#ip rsvp bandwidth 140000 140000\     |
                     sub-pool 70000                         |
router-3(config-subif)# mpls traffic-eng tunnels           |
router-3(config-subif)# atm pvc 10 10 100 aal5snap         |
[if using IS-IS instead of OSPF]:                           |
router-3(config-subif)# ip router isis                     |
router-3(config-subif)# exit                               |
```

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
```

[and in all cases]:

```
router-3(config-if)# exit
```

At the outgoing network interface through which two global pool tunnels currently exit:

[ATM-PVC case appears on the left; POS case on the right]:

```
router-3(config)# interface atm7/2                          | interface POS4/1
```

[then continue each case at the network interface level:

```
router-3(config-if)# mpls traffic-eng tunnels              | ip address 13.1.1.1 255.0.0.0
router-3(config-if)# ip rsvp bandwidth 140000 140000\       | mpls traffic-eng tunnels
                     sub-pool 70000                         |
router-3(config-if)# interface atm7/2.0                    | ip rsvp bandwidth 140000 140000\
                                                            |    sub-pool 70000
router-3(config-subif)# ip address 13.1.1.1 255.0.0.0      |
router-3(config-subif)#ip rsvp bandwidth 140000 140000\     |
                     sub-pool 70000                         |
router-3(config-subif)# mpls traffic-eng tunnels           |
router-3(config-subif)# atm pvc 10 10 100 aal5snap         |
[if using IS-IS instead of OSPF]:                           |
router-3(config-subif)# ip router isis                     |
router-3(config-subif)# exit                               |
```

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-3(config-if)# ip router isis
```

[and in all cases]:

```
router-3(config-if)# exit
```

Tunnel Midpoint Configuration [Mid-2]

[For the sake of simplicity, only the POS example (Figure 8) is illustrated with a second midpoint router.] Both interfaces on this midpoint router are configured like the outbound interfaces of the Mid-1 router.

Configuring the Pools and Tunnels

At the device level:

```
router-5(config)# ip cef
router-5(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-5(config)# **router isis**	**router ospf 100**
router-5(config-router)# **net 49.2500.1000.0000.0012.00**	**redistribute connected**
router-5(config-router)# **metric-style wide**	**network 13.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **is-type level-1**	**network 14.1.1.0 0.0.0.255 area 0**
router-5(config-router)# **mpls traffic-eng level-1**	**network 25.1.1.1 0.0.0.0 area 0**
router-5(config-router)#	**mpls traffic-eng area 0**

[now one resumes the common command set]:

```
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit
```

Create a virtual interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit
```

At the incoming network interface:

```
router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
```

[and if using IS-IS instead of OSPF]:

```
router-5(config-if)# ip router isis
```

[and in all cases]:

```
router-5(config-if)# exit
```

At the outgoing network interface:

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
```

[and if using IS-IS instead of OSPF]:

```
router-5(config-if)# ip router isis
```

[and in all cases]:

```
router-5(config-if)# exit
```

Tunnel Tail Configuration

The inbound interfaces on the tail router are configured much like the outbound interfaces of the midpoint routers:

Configuring the Pools and Tunnels

At the device level:

```
router-4(config)# ip cef
router-4(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right. In the case of OSPF, one must advertise two new loopback interfaces—29.1.1.1 and 30.1.1.1 in our example—which are defined in the QoS Policy Propagation section, further along on this page]:

router-4(config)# **router isis**	**router ospf 100**
router-4(config-router)# **net 49.0000.2700.0000.0000.00**	**redistribute connected**

```
router-4(config-router)# metric-style wide              network 12.1.1.0 0.0.0.255 area 0
router-4(config-router)# is-type level-1                network 14.1.1.0 0.0.0.255 area 0
router-4(config-router)# mpls traffic-eng level-1       network 27.1.1.1 0.0.0.0 area 0
router-4(config-router)#                                network 29.1.1.1 0.0.0.0 area 0
router-4(config-router)#                                network 30.1.1.1 0.0.0.0 area 0
router-4(config-router)#                                mpls traffic-eng area 0
```

[now one resumes the common command set, taking care to include the two additional loopback interfaces]:

```
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# mpls traffic-eng router-id Loopback1
router-4(config-router)# mpls traffic-eng router-id Loopback2
router-4(config-router)# exit
```

Create a virtual interface:

```
router-4(config)# interface Loopback0
router-4(config-if)# ip address 27.1.1.1 255.255.255.255
router-4(config-if)# exit
```

At one incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

```
router-4(config)# interface atm8/1                          interface POS2/1
```

[then continue each case at the network interface level:

```
router-4(config-if)# mpls traffic-eng tunnels               ip address 12.1.1.2 255.0.0.0
router-4(config-if)# ip rsvp bandwidth 140000 140000\       mpls traffic-eng tunnels
                     sub-pool 70000
router-4(config-if)# interface atm8/1.2                     ip rsvp bandwidth 140000 140000\
                                                               sub-pool 70000
router-4(config-subif)# ip address 12.1.1.2 255.0.0.0
router-4(config-subif)#ip rsvp bandwidth 140000 140000\
                     sub-pool 70000
router-4(config-subif)# mpls traffic-eng tunnels
router-4(config-subif)# atm pvc 10 10 100 aal5snap
[if using IS-IS instead of OSPF]:
router-4(config-subif)# ip router isis
router-4(config-subif)# exit
```

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-4(config-if)# ip router isis
```

[and in all cases]:

```
router-4(config-if)# exit
```

At the other incoming network interface:

[ATM-PVC case appears on the left; POS case on the right]:

```
router-4(config)# interface atm8/1                          interface POS2/2
```

[then continue each case at the network interface level:

```
router-4(config-if)# mpls traffic-eng tunnels               ip address 14.1.1.2 255.0.0.0
router-4(config-if)# ip rsvp bandwidth 140000 140000\       mpls traffic-eng tunnels
                     sub-pool 70000
router-4(config-if)# interface atm8/1.2                     ip rsvp bandwidth 140000 140000\
                                                               sub-pool 70000
router-4(config-subif)# ip address 14.1.1.2 255.0.0.0
router-4(config-subif)#ip rsvp bandwidth 140000 140000\
                     sub-pool 70000
```

```
router-4(config-subif)# mpls traffic-eng tunnels
router-4(config-subif)# atm pvc 10 10 100 aal5snap
```

[if using IS-IS instead of OSPF]:

```
router-4(config-subif)# ip router isis
router-4(config-subif)# exit
```

Continuing at the network interface level, regardless of interface type:

[If using IS-IS instead of OSPF]:

```
router-4(config-if)# ip router isis
```

[and in all cases]:

```
router-4(config-if)# exit
```

Configuring QoS Policy Propagation

On the tail device, one must configure a separate virtual loopback IP address for each class-of-service terminating here. The headend routers need these addresses to map traffic into the proper tunnels. In the current example, four tunnels terminate on the same tail device but they represent only two service classes, so only two additional loopback addresses are needed:

Create two virtual interfaces:

```
router-4(config)# interface Loopback1
router-4(config-if)# ip address 29.1.1.1 255.255.255.255
```

[and if using IS-IS instead of OSPF]:

```
router-4(config-if)# ip router isis
```

[and in all cases]:

```
router-4(config-if)# exit
router-4(config)# interface Loopback2
router-4(config-if)# ip address 30.1.1.1 255.255.255.255
```

[and if using IS-IS instead of OSPF]:

```
router-4(config-if)# ip router isis
```

[and in all cases]:

```
router-4(config-if)# exit
```

At the device level, configure BGP to send the community to each tunnel head:

```
router-4(config)# router bgp 2
router-4(config-router)# neighbor 23.1.1.1 send-community
router-4(config-router)# neighbor 22.1.1.1 send-community
router-4(config-router)# exit
```

Command Reference

The following commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm.

- **debug mpls traffic-engineering link-management preemption**
- **extended-port**
- **interface**
- **ip cef**
- **ip router isis**
- **ip rsvp bandwidth**
- **is-type**
- **metric-style wide**
- **mpls traffic-eng**
- **mpls traffic-eng administrative-weight**
- **mpls traffic-eng area**
- **mpls traffic-eng atm cos global-pool**
- **mpls traffic-eng atm cos sub-pool**
- **mpls traffic-eng attribute-flags**
- **mpls traffic-eng backup-path tunnel**
- **mpls traffic-eng flooding thresholds**
- **mpls traffic-eng link timers bandwidth-hold**
- **mpls traffic-eng link timers periodic-flooding**
- **mpls traffic-eng reoptimize timers frequency**
- **mpls traffic-eng router-id**
- **mpls traffic-eng tunnels (configuration)**
- **mpls traffic-eng tunnels (interface)**
- **net**
- **passive-interface**
- **router isis**
- **router ospf**
- **show interfaces tunnel**
- **show ip ospf**
- **show ip route**
- **show ip rsvp host**
- **show ip rsvp interface**
- **show mpls traffic-eng autoroute**
- **show mpls traffic-eng fast-reroute database**

- **show mpls traffic-eng fast-reroute log reroutes**
- **show mpls traffic-eng link-management admission-control**
- **show mpls traffic-eng link-management advertisements**
- **show mpls traffic-eng link-management bandwidth-allocation**
- **show mpls traffic-eng link-management igp-neighbors**
- **show mpls traffic-eng link-management interfaces**
- **show mpls traffic-eng link-management summary**
- **show mpls traffic-eng topology**
- **show mpls traffic-eng tunnels**
- **mpls atm vpi**
- **tunnel destination**
- **tunnel mode mpls traffic-eng**
- **tunnel mpls traffic-eng affinity**
- **tunnel mpls traffic-eng autoroute announce**
- **tunnel mpls traffic-eng autoroute metric**
- **tunnel mpls traffic-eng bandwidth**
- **tunnel mpls traffic-eng fast-reroute**
- **tunnel mpls traffic-eng path-option**
- **tunnel mpls traffic-eng priority**

Glossary

This section defines acronyms and words that may not be readily understood.

AS—Autonomous System. A collection of networks under a common administration, sharing a common routing strategy and identified by a unique 16-bit number (assigned by the Internet Assigned Numbers Authority).

ATM—Asynchronous Transfer Mode. The international standard for cell relay in which several service types (such as voice, video or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

BGP—Border Gateway Protocol. The predominant interdomain routing protocol. It is defined by RFC 1163. Version 4 uses route aggregation mechanisms to reduce the size of routing tables.

BPX—A Cisco standards-based ATM switch that supports broadband, narrowband, and IP services.

CBR—Constraint Based Routing. The computation of traffic paths that simultaneously satisfy label-switched path attributes and current network resource limitations.

CEF—Cisco Express Forwarding. A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

CLI—Command Line Interface. Cisco's interface for configuring and managing its routers.

DS-TE—Diff Serv-aware Traffic Engineering. The capability to configure two bandwidth pools on each link, a *global pool* and a *sub-pool*. MPLS traffic engineering tunnels using the sub-pool bandwidth can be configured with Quality of Service mechanisms to deliver guaranteed bandwidth services end-to-end across the network. Simultaneously, tunnels using the global pool can convey diff-serv traffic.

flooding—A traffic passing technique used by switches and bridges in which traffic received on an interface is sent out through all of the interfaces of that device except the interface on which the information was originally received.

GB queue—Guaranteed Bandwidth queue. A per-hop behavior (PHB) used exclusively by the strict guarantee traffic. If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used.

Global Pool—The total bandwidth allocated to an MPLS traffic engineering link.

IGP—Interior Gateway Protocol. An internet protocol used to exchange routing information within an autonomous system. Examples of common internet IGPs include IGRP, OSPF, and RIP.

label-switched path (LSP) tunnel—A configured connection between two routers, using label switching to carry the packets.

IS-IS—Intermediate System-to-Intermediate System. A link-state hierarchical routing protocol, based on DECnet Phase V routing, whereby nodes exchange routing information based on a single metric, to determine network topology.

LCAC—Link-level (per-hop) call admission control.

LC-ATM—Label switching Controlled ATM. The assignment of values into the VPI/VCI field of ATM cells by MPLS rather than by ATM control procedures.

LSP—Label-switched path (see above).
Also Link-state packet—A broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSPs are used by the receiving routers to maintain their routing tables. Also called link-state advertisement (LSA).

MPLS—Multi-Protocol Label Switching (formerly known as Tag Switching). A method for directing packets primarily through Layer 2 switching rather than Layer 3 routing, by assigning the packets short fixed-length labels at the ingress to an MPLS cloud, using the concept of forwarding equivalence classes. Within the MPLS domain, the labels are used to make forwarding decisions mostly without recourse to the original packet headers.

MPLS TE—MPLS Traffic Engineering (formerly known as "RRR" or Resource Reservation Routing). The use of label switching to improve traffic performance along with an efficient use of network resources.

OSPF—Open Shortest Path First. A link-state, hierarchical IGP routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

POS—Packet over SONET (Synchronous Optical Network).

PVC—Permanent Virtual Connection. A circuit or channel through an ATM network provisioned by a carrier between two end points; used for dedicated long-term information transport between locations. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time.

RSVP—Resource reSerVation Protocol. An IETF protocol used for signaling requests (to set aside internet services) by a customer before that customer is permitted to transmit data over that portion of the network.

Sub-pool—The more restrictive bandwidth in an MPLS traffic engineering link. The sub-pool is a portion of the link's overall global pool bandwidth.

TE—Traffic engineering. The application of scientific principles and technology to measure, model, and control internet traffic in order to simultaneously optimize traffic performance and network resource utilization.

Configuring the Multiprotocol over ATM Client

This chapter describes the required and optional tasks for configuring the Multiprotocol over ATM (MPOA) client (MPC).

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."

The MPC functionality involves ingress/egress cache management, data-plane and control-plane virtual circuit connection (VCC) management, MPOA frame processing, and participation in MPOA protocol and MPOA flow detection.

How MPC Works

The MPC software module implements the functionality of the MPC in compliance with the ATM Forum MPOA specification. An MPC identifies packets sent to an MPOA-capable router over the nonbroadcast multi-access (NBMA) network and establishes a shortcut VCC to the egress MPC, if possible. The MPC then routes these packets directly over this shortcut VCC, bypassing the intermediate routers and enabling the fast routing of internetwork-layer packets across an NBMA network. The Catalyst 5000 series switch can be designated as an MPC. If the Catalyst 5000 series switch is configured with an RSM/VIP2 (with an ATM interface) it can be configured as an MPC or an MPS.

A router is usually designated as an MPOA server (MPS), but can also be designated as an MPC. MPC on the router is primarily meant to provide router-initiated and router-terminated shortcuts for non-NBMA networks. For this reason, MPC information in this chapter primarily refers to the Catalyst 5000 series switch, and MPS information refers to the router or the RSM/VIP2 with an ATM interface in a Catalyst 5000 series switch.

MPC Configuration Task List

To configure an MPC on your network, perform the tasks described in the following sections. The first two sections contain required tasks; the remaining tasks are optional:

- Configuring the ELAN ID (Required)

- Configuring the MPC (Required)
- Configuring the MPC Variables (Optional)
- Monitoring and Maintaining the MPC (Optional)

Configuring the ELAN ID

For MPOA to work properly, a LEC must belong to an ELAN that has a defined ELAN ID. To obtain an ELAN ID, use either of the following commands in LANE database configuration mode:

Note To configure an MPC on a Catalyst 5000 series ATM module, establish connection with the ATM module, enter privileged mode, and then enter configuration mode. For information on performing these tasks, refer to the *Catalyst 5000 Series Software Configuration Guide*.

Command	Purpose
Router(lane-config-dat)# **name** *elan-name* **elan-id** *id*	Defines an ELAN ID for the LEC (in LANE database configuration mode).
Router(lane-config-dat)# **lane server-bus ethernet** *elan-name* [**elan-id** *id*]	Configures the LEC with the ELAN ID (in interface configuration mode).

Caution If an ELAN ID is supplied, make sure both commands use the same elan-id value.

Configuring the MPC

To configure an MPC on your network, use the following commands in beginning in global configuration modes:

	Command	Purpose
Step 1	Router(config)# **mpoa client config name** *mpc-name*	In global configuration mode, defines an MPC with a specified name.
Step 2	Router(config-if)# **interface atm** {*mod-num/port-num* | *number*}	In interface configuration mode, specifies the ATM interface to which the MPC is associated.
Step 3	Router(config-if)# **mpoa client name** *mpc-name*	In interface configuration mode, attaches an MPC to the ATM interface.
Step 4	Router(config-if)# **interface** *atm-num.sub-interface-num*	In interface configuration mode, specifies the ATM interface that contains the LEC to which you will bind the MPC.
Step 5	Router(config-if)# **lane client mpoa client name** *mpc-name*	In interface configuration mode, binds a LEC to the specified MPC.
	Repeat Steps 4 and 5 for every LEC to be served by the MPC/MPS.	

Configuring the MPC Variables

An MPC has to be defined with a specified name before you can change its variables.

To change the variables for an MPC, use the following commands in MPC configuration mode:

	Command	Purpose
Step 1	`Router(mpoa-client-config)#` **mpoa client config name** *mps-name*	Defines an MPC with the specified name.
Step 2	`Router(mpoa-client-config)#` **atm-address** *atm-address*	(Optional) Specifies the control ATM address that the MPC should use (when it is associated with a hardware interface).
Step 3	`Router(mpoa-client-config)#` **shortcut-frame-count** *count*	(Optional) Specifies the maximum number of times a packet can be routed to the default router within shortcut-frame time before an MPOA resolution request is sent.
Step 4	`Router(mpoa-client-config)#` **shortcut-frame-time** *time*	(Optional) Sets the shortcut-setup frame time for the MPC.

Monitoring and Maintaining the MPC

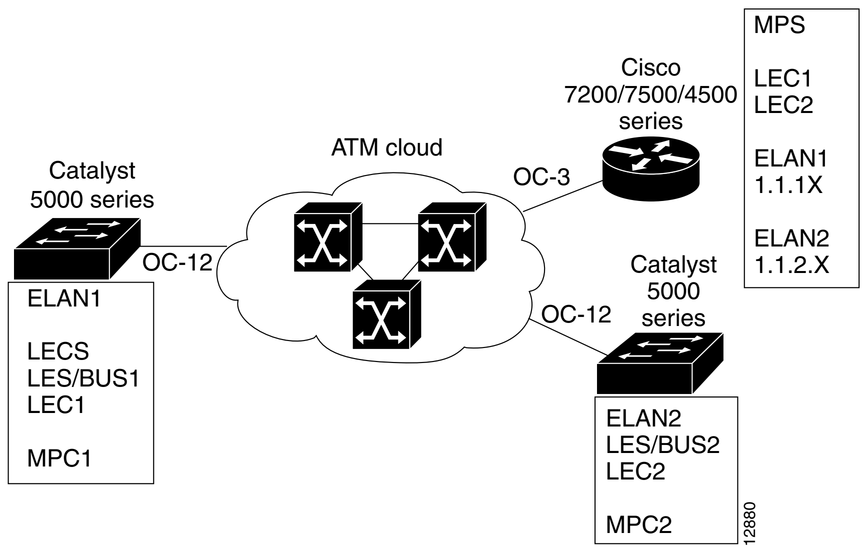
To monitor and maintain the configuration of an MPC, use the following commands in EXEC mode, as needed:

Command	Purpose
`Router#` **show mpoa client** [**name** *mpc-name*]	Displays information about a specified MPC or all MPCs.
`Router#` **show mpoa client** [**name** *mpc-name*] **cache** [**ingress** | **egress**] [**ip-addr** *ip-addr*]	Displays ingress and egress cache entries associated with an MPC.
`Router#` **show mpoa client** [**name** *mpc-name*] **statistics**	Displays all the statistics collected by an MPC.
`Router#` **clear mpoa client** [**name** *mpc-name*] **cache** [**ingress** | **egress**] [**ip-addr** *ip-addr*]	Clears cache entries.
`Router#` **show mpoa client** [**name** *mpc-name*] [*remote-device*]	Displays all the MPOA devices that this MPC has learned.
`Router#` **show mpoa default-atm-addresses**	Displays the default ATM addresses for the MPC.

MPC Configuration Example

This section contains an example of the commands needed to configure an MPC. The lines beginning with exclamation points (!) are comments explaining the command shown on the subsequent line. Figure 34 shows an example of how you can configure your system to use MPOA.

Figure 34 Example of an MPOA Configuration



The following example configures the MPC and attaches the MPC to a hardware interface:

```
! Define the MPC "MYMPC"
 mpoa client config name MYMPC
! Leave everything as default
 exit
! Specify the ATM interface to which the MPC is attached
 interface ATM 1/0
! Attach MPC MYMPC to the HW interface
 mpoa client name MYMPC
! Specify the ATM interface that contains the LEC to which you will bind the MPC
 interface atm 1/0.1
! Bind a LANE client to the specified MPC
 lane client mpoa client name MYMPC
! Go back up to global config mode
 exit
```

The following example shows a typical configuration file for the first MPC:

```
Current configuration:
!
version 11.3
! Go to LANE database config mode
 exit
lane database mpoa-test
hostname mpc-1
! Define the ELAN ID and ATM address
name elan1 server-atm-address 47.00918100000000613E5A2F01.006070174821.01
name elan1 elan-id 101
name elan2 server-atm-address 47.00918100000000613E5A2F01.006070174821.02
name elan2 elan-id 102
! Define the MPC "mpc-1"
```

```
mpoa client config name mpc-1
    interface Ethernet0
! Go back up to global config mode
 exit
! Specify the ATM interface to which the MPC is attached
interface ATM0
    atm pvc 1 0 5 qsaal
    atm pvc 2 0 16 ilmi
    lane config auto-config-atm-address
    lane config database mpoa-test
! Attach MPC mpc-1 to the HW interface
    mpoa client name mpc-1
! Specify the ATM interface that contains the LEC to which you will bind the MPC
interface ATM0.1 multipoint
    lane server-bus ethernet elan1
! Bind a LANE client to the specified MPC
    lane client mpoa client name mpc-1
    lane client ethernet 1 elan1
! Go back up to global config mode
 exit
```

The following example shows a typical configuration file for the second MPC:

```
Current configuration:
!
version 11.3
hostname mpc-2
! Go back up to global config mode
 exit
! Define the MPC "mpc-2"
mpoa client config name mpc-2
! Specify the ATM interface to which the MPC is attached
interface ATM0
    atm pvc 1 0 5 qsaal
    atm pvc 2 0 16 ilmi
    mpoa client name mpc-2
! Specify the ATM interface that contains the LEC to which you will bind the MPC
interface ATM0.1 multipoint
    lane server-bus ethernet elan2
    lane client mpoa client name mpc-2
    lane client ethernet 2 elan2
! Go back up to global config mode
 exit
```

Configuring the Multiprotocol over ATM Server

This chapter describes the required and optional tasks for configuring the Multiprotocol over ATM (MPOA) server (MPS).

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."

The MPS supplies the forwarding information used by the MPOA clients (MPCs). The MPS responds with the information after receiving a query from a client. To support the query and response functions, MPOA has adopted the Next Hop Resolution Protocol (NHRP). The MPS on the router can also terminate shortcuts.

How MPS Works

The MPS software module implements the functionality of the MPS in compliance with the ATM Forum MPOA specification. The following sections describe the functions of MPS:

- MPS-NHRP-Routing Interaction
- Shortcut Domains

MPS-NHRP-Routing Interaction

MPS must interact with the NHRP module in the router to smoothly propagate MPOA/NHRP packets end to end. MPOA frames are identical to NHRP frames except for some specific op-codes and extensions for MPOA.

The following process explains the interaction of MPS and NHRP:

1. MPS converts MPOA resolution requests to NHRP requests and sends it either to the next hop MPS or to the Next Hop Server (NHS), depending on the configuration. MPS searches for the next hop routing information to determine the interface and sends the packet with correct encapsulation to an MPS or an NHS.

2. NHS sends resolution requests to MPS when the next hop is on a LAN Emulation (LANE) cloud or when NHS is unsure of the packet destination. MPS may do further processing, such as prompt NHS to terminate the request or throw away the packet.
3. NHS sends resolution replies to MPS when the next hop interface is LANE or when the replies terminate in the router. Then MPS sends an MPOA resolution reply to the MPC.

Shortcut Domains

Within a router, it is possible to permit shortcuts between one group of LAN Emulation Clients (LECs) and deny it between some other groups of LECs. Cisco introduces a notion of network ID associated with an MPS. By default, all the MPSs in a router get a network ID of 1.

If the administrator wants to segregate traffic, then MPSs can be given different network IDs, in effect preventing shortcuts between LECs served by different MPSs. This can be configured in the definition of an MPS database.

If a router has both MPS and NHRP configured, then the same network ID is required to facilitate requests, replies, and shortcuts across the MPS and NHRP. The interface-specific NHRP command (**ip nhrp network-id**) must be the same for an MPS; otherwise, there will be a disjointed network.

MPS Configuration Task List

To configure an MPS on your network, perform the following tasks:

- Configuring the ELAN ID (Required)
- Configuring the MPS (Required)
- Configuring the MPS Variables (Optional)
- Monitoring and Maintaining the MPS (Optional)

Configuring the ELAN ID

For MPOA to work properly, a LANE client must have an ELAN ID for all ELANs represented by the LANE clients. To configure an ELAN ID, use either of the following commands in lane database configuration mode or in interface configuration mode when starting up the LAN Emulation Client Server (LECS) for that ELAN:

Command	Purpose
`Router(lane-config-dat)#` **name** *elan-name* **elan-id** *id*	Configures the ELAN ID in the LECS database to participate in MPOA.
`Router(lane-config-dat)#` **lane server-bus** {**ethernet** | **tokenring**} *elan-name* [**elan-id** *id*]	Configures the LAN Emulation Server (LES) with the ELAN ID to participate in MPOA.

Caution If an ELAN ID is supplied by both commands, make sure that the ELAN ID matches in both.

Configuring the MPS

To configure an MPS, use the following commands beginning in global configuration mode. The MPS starts functioning only after it is attached to a specific hardware interface:

	Command	Purpose
Step 1	`Router(config)#` **`mpoa server config name`** *`mps-name`*	In global configuration mode, defines an MPS with the specified name.
Step 2	`Router(config)#` **`interface atm`** `{`*`slot/port`* `|` *`number`*`}`	Specifies the ATM interface to attach the MPS.
Step 3	`Router(config-if)#` **`mpoa server name`** *`mps-name`*	In interface configuration mode, attaches the MPS to the ATM interface.
Step 4	`Router(config-if)#` **`interface atm`** `{`*`slot/port.subinterface-number`* `|` *`number.subinterface-number`*`}`	Specifies the ATM interface to bind the MPS to a LEC.
Step 5	`Router(config-subif)#` **`lane client mpoa server name`** *`mps-name`*	In subinterface configuration mode, binds a LANE client to the specified MPS.

Configuring the MPS Variables

An MPS must be defined with a specified name before you can change the MPS variables specific to that MPS.

To change MPS variables specific only to a particular MPS, use the following commands beginning in MPS configuration mode:

	Command	Purpose
Step 1	`Router(mpoa-server-config)#` **`mpoa server config name`** *`mps-name`*	Defines an MPS with the specified name.
Step 2	`Router(mpoa-server-config)#` **`atm-address`** *`atm-address`*	(Optional) Specifies the control ATM address that the MPS should use (when it is associated with a hardware interface).
Step 3	`Router(mpoa-server-config)#` **`holding-time`** *`time`*	(Optional) Specifies the holding time value for the MPS-p7 variable of the MPS.
Step 4	`Router(mpoa-server-config)#` **`keepalive-lifetime`** *`time`*	(Optional) Specifies the keepalive lifetime value for the MPS-p2 variable of the MPS.
Step 5	`Router(mpoa-server-config)#` **`keepalive-time`** *`time`*	(Optional) Specifies the keepalive time value for the MPS-p1 variable of the MPS.
Step 6	`Router(mpoa-server-config)#` **`network-id`** *`id`*	(Optional) Specifies the network ID of the MPS.

Monitoring and Maintaining the MPS

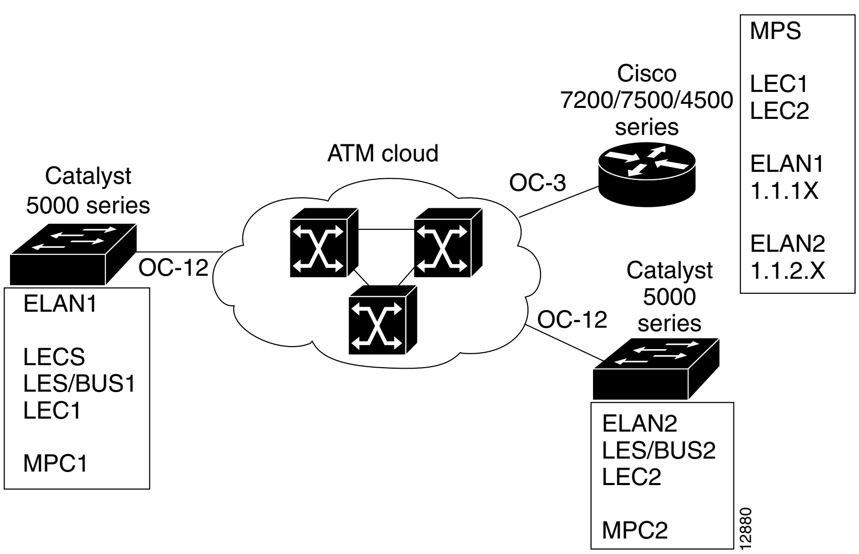
To monitor and maintain the configuration of an MPS, use the following commands in EXEC mode, as needed:

Command	Purpose
`Router# show mpoa default-atm-addresses`	Displays default ATM addresses for an MPS.
`Router# show mpoa server [name mps-name]`	Displays information about a specified server or all servers depending on the specified name of the required server.
`Router# show mpoa server [name mps-name] cache [ingress | egress] [ip-address ip-address]`	Displays ingress and egress cache entries associated with a server.
`Router# show mpoa server [name mps-name] statistics`	Displays all the statistics collected by a server including the ingress and egress cache entry creations, deletions, and failures.
`Router# clear mpoa server [name mps-name] cache [ingress | egress] [ip-addr ip-addr]`	Clears cache entries.
`Router# mpoa server name mps-name trigger ip-address ip-address [mpc-address mpc-address]`	Originates an MPOA trigger for the specified IP address to the specified client. If a client is not specified, the MPOA is triggered to all the clients.

MPS Configuration Example

This section contains an example of the commands needed to configure an MPS. The lines beginning with exclamation points (!) are comments explaining the command shown on the following line. Figure 35 shows an example of how you can configure your system to utilize MPOA.

Figure 35 Example of an MPOA Configuration



The following example configures the MPS and attaches the MPS to a hardware interface:

```
! Define the MPS “MYMPS”
 mpoa server config name MYMPS
! Leave everything as default
 exit
! Enter into interface config mode
 interface ATM 1/0
! Attach MPS MYMPS to the HW interface
 mpoa server name MYMPS
! Go back up to global config mode
 exit
```

The following example shows a typical MPS configuration file:

```
version 11.3
hostname MPS
! Define the MPS “mps”
mpoa server config name mps
! Specify the ATM interface to which the MPS is attached
interface ATM4/0
    no ip address
    atm pvc 1 0 5 qsaal
    atm pvc 2 0 16 ilmi
    lane config auto-config-atm-address
    mpoa server name mps
! Specify the ATM interface that contains the LEC to which you will bind the MPS
interface ATM4/0.1 multipoint
    ip address 1.1.1.2 255.255.255.0
    lane client mpoa server name mps
    lane client ethernet elan1
interface ATM4/0.2 multipoint
    ip address 1.1.2.1 255.255.255.0
    lane client mpoa server name mps
    lane client ethernet elan2
end
```

Configuring Token Ring LAN Emulation for Multiprotocol over ATM

This chapter describes the required and optional tasks for configuring the MPOA for Token Ring Networks feature.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

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."

The MPOA for Token Ring Networks feature allows Token Ring hosts on an ATM network to communicate over direct paths (called shortcuts) through the ATM network. These shortcuts bypass the intermediate router hops that otherwise would be encountered in the default path.

How Token Ring MPOA Works

Token Ring Multiprotocol over ATM (MPOA) is an extension to LAN Emulation (LANE). It allows Token Ring LANE clients to forward IP packets between subnets to other Token Ring LANE clients through a shortcut in the ATM network. The Token Ring LANE clients have an MPOA client (MPC) communicating with an MPOA server (MPS) to establish this shortcut.

Token Ring LANE for MPOA Configuration Task List

To configure Token Ring LANE for MPOA, perform the tasks described in the following sections:

- Configuring a Token Ring LEC
- Configuring the LECS Database
- Configuring the LES/BUS

Configuring a Token Ring LEC

For MPOA operation, a LEC must be associated with an MPS, an MPC, or both. Once a LEC is bound to a particular MPS/MPC, it cannot be bound to another MPS/MPC at the same time.

The LEC must also be associated with a physical interface or subinterface, which may be different from the physical interface associated with the MPS or MPC. For proper operation, all interfaces must belong to the same ATM network.

To configure a Token Ring LEC, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **interface atm** {*slot***/***port***.***subinterface-number* | *number***.***subinterface-number*}	Specifies the ATM interface to be associated with the LEC.
Step 2	Router(config-if)# **lane client tokenring** [*elan-name*]	Defines a Token Ring LEC on a specified ELAN name.
Step 3	Router(config-if)# **lane client mpoa server** *mps-name*	(Optional) Binds a Token Ring LEC to an MPS.
Step 4	Router(config-if)# **lane client mpoa client** *mpc-name*	(Optional) Binds a Token Ring LEC to an MPC.

Configuring the LECS Database

To configure the LECS database, use the following commands in beginning global configuration mode:

	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*	Binds the name of the ELAN to the ATM address of the LES.
Step 3	Router(lane-config-dat)# **name** *elan-name* **elan-id** *id*	Defines the ELAN ID in the LECS database to participate in MPOA.
Step 4	Router(lane-config-dat)# **name** *elan-name* **local-seg-id** *id*	Configures the local segment ID number.

Configuring the LES/BUS

To configure the LES/BUS, use the following commands in beginning global configuration mode:

	Command	Purpose
Step 1	Router(config)# **interface atm** {*slot***/***port***.***subinterface-number* | *number***.***subinterface-number*}	Specifies the ATM subinterface to be associated with the LES/BUS.
Step 2	Router(config-if)# **lane server-bus tokenring** *elan-name* [**elan-id** *elan-id*]	Defines a Token Ring LES/BUS on the named ELAN. The ELAN ID is optional.

Token Ring LANE Configuration Examples

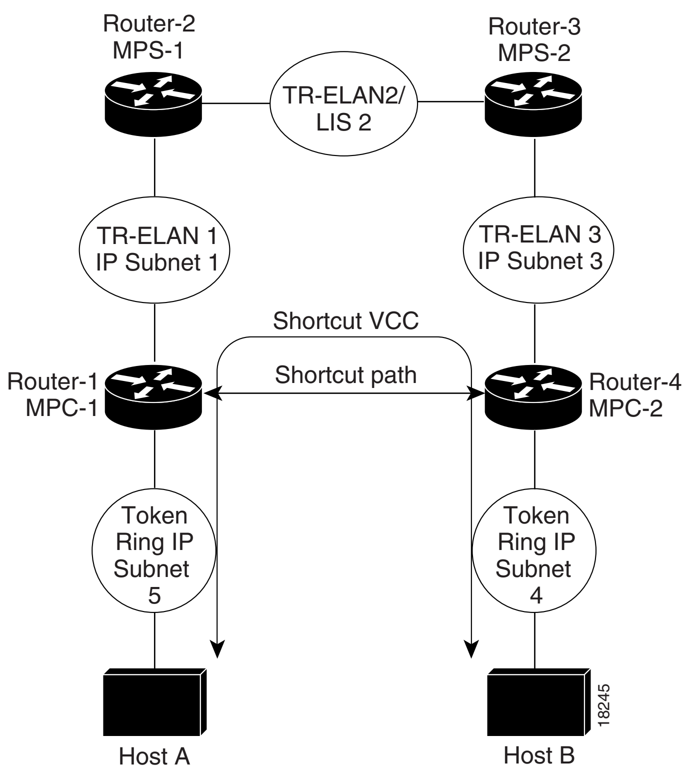
This section provides the following sample configurations of MPOA in a Token Ring LANE environment:

- MPOA Token Ring LANE Configuration in an IP-Routed Domain Example
- MPOA Token Ring LANE Configuration in an IP SRB-Routed Domain Example

MPOA Token Ring LANE Configuration in an IP-Routed Domain Example

Figure 36 illustrates MPOA in a Token Ring LANE environment where MPC-to-MPC shortcuts are established between Token Ring LANE edge routers that reside in different IP-routed domains.

Figure 36 Token Ring MPOA—MPC to MPC Shortcut in an IP Routed Environment



The following commands show a sample configuration for Router-1 in Figure 36:

```
hostname Router-1
!
ip routing
!
! Define the MPOA Client (mpc-1) configuration.
!
mpoa client config name mpc-1
!
! Configure an IP address on the Token Ring interface.
!
```

```
interface TokenRing1/0
 ip address 5.5.5.2 255.255.255.0
 ring-speed 16
!
! Configure a config-server and bind it to its database (mpoa-db).
! Attach the MPOA client mpc-1 to its ATM interface.
!
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database mpoa-db
 mpoa client name mpc-1
!
! Configure a LANE server-bus and LANE client on ELAN 1. Bind the
! LANE client to its MPOA Client (mpc-1).
!
interface ATM2/0.1 multipoint
 ip address 1.1.1.1 255.255.255.0
 lane server-bus tokenring 1
 lane client mpoa client name mpc-1
 lane client tokenring 1
!
router eigrp 1
 network 1.0.0.0
 network 5.0.0.0
!
end
```

The following commands show a sample configuration for Router-2 in Figure 36:

```
hostname Router-2
!
ip routing
!
! Configure the config-server database mpoa-db with configuration
! for ELANs 1 to 3
!
lane database mpoa-db
 name 1 server-atm-address 47.00918100000000060705BFA01.00000CA05F41.01
 name 1 local-seg-id 1000
 name 1 elan-id 100
 name 2 server-atm-address 47.00918100000000060705BFA01.00000CA05B41.01
 name 2 local-seg-id 2000
 name 2 elan-id 200
 name 3 server-atm-address 47.00918100000000060705BFA01.00000CA05B41.03
 name 3 local-seg-id 3000
 name 3 elan-id 300
!
! Define the MPOA Server (mps-1) configuration.
mpoa server config name mps-1
!
! Configure the signalling and ILMI PVCs. Also configure a config-server
! and attach the MPOA server (mps-1) to its ATM interface.
!
interface ATM4/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 lane config auto-config-atm-address
 lane config database mpoa-db
 mpoa server name mps-1
!
! Configure a Token Ring LANE client on ELAN 1 and bind the LANE
```

```
! client to its MPOA server (mps-1).
!
interface ATM4/0.1 multipoint
 ip address 1.1.1.2 255.255.255.0
 lane client mpoa server name mps-1
 lane client tokenring 1
!
! Configure a Token Ring LANE client on ELAN 2 and bind the LANE
! client to its MPOA server (mps-1)
!
interface ATM4/0.2 multipoint
 ip address 2.2.2.1 255.255.255.0
 lane client mpoa server name mps-1
 lane client tokenring 2
!
router eigrp 1
 network 1.0.0.0
 network 2.0.0.0
!
end
```

The following commands show a sample configuration for Router-3 in Figure 36:

```
hostname Router-3
!
ip routing
!
! Defines the MPOA Server (mps-2) configuration.
mpoa server config name mps-2
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! server (mps-2) to its ATM interface.
!
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 mpoa server name mps-2
!
! Configure a Token Ring LANE client and LANE server-bus on ELAN 2
! and bind the LANE client to its MPOA server (mps-2)
!
interface ATM2/0.1 multipoint
 ip address 2.2.2.2 255.255.255.0
 lane server-bus tokenring 2
 lane client mpoa server name mps-2
 lane client tokenring 2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA server (mps-2)
!
interface ATM2/0.3 multipoint
 ip address 3.3.3.1 255.255.255.0
 lane server-bus tokenring 3
 lane client mpoa server name mps-2
 lane client tokenring 3
!
router eigrp 1
 network 2.0.0.0
 network 3.0.0.0
!
end
```

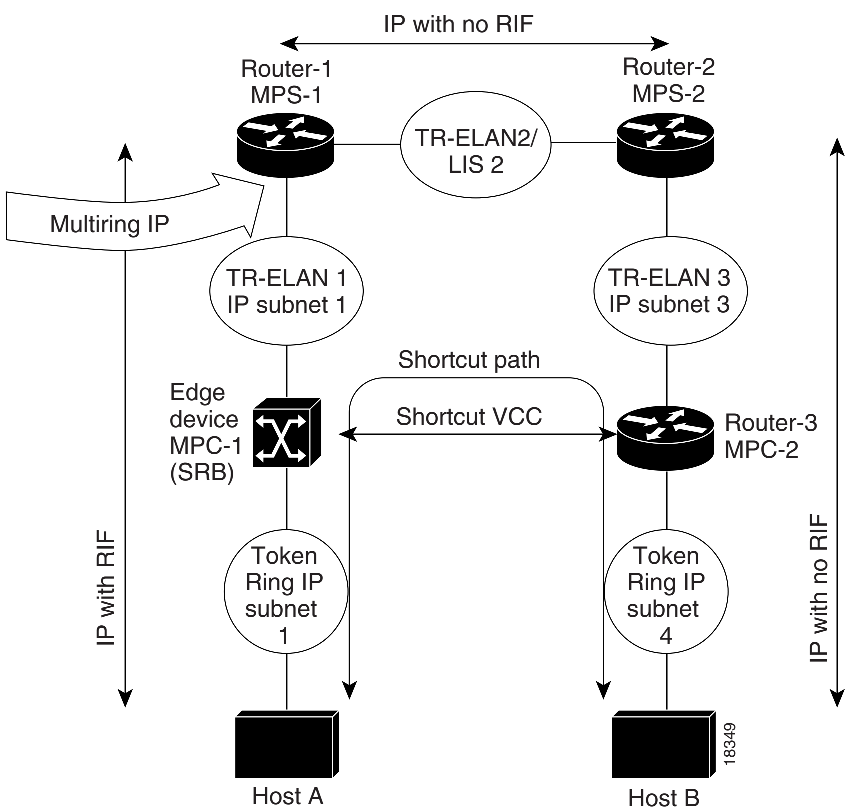
The following commands show a sample configuration for Router-4 in Figure 36:

```
hostname Router-4
!
ip routing
!
! Define the MPOA client (mpc-2) configuration.
!
mpoa client config name mpc-2
!
! Configure the Token Ring interface
!
interface TokenRing1/0
 ip address 4.4.4.1 255.255.255.0
 ring-speed 16
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! client to its ATM interface.
!
interface ATM2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 mpoa client name mpc-2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA client (mpc-2).
!
interface ATM2/0.1 multipoint
 ip address 3.3.3.2 255.255.255.0
 lane client mpoa client name mpc-2
 lane client tokenring 3
!
router eigrp 1
 network 3.0.0.0
 network 4.0.0.0
!
end
```

MPOA Token Ring LANE Configuration in an IP SRB-Routed Domain Example

Figure 37 illustrates MPOA in a Token Ring LANE environment where MPC-to-MPC shortcuts are established between a Token Ring LANE edge device and a Token Ring LANE router that reside in an IP SRB domain and IP-routed domains.

Figure 37 Token Ring MPOA—MPC to MPC Shortcut in an IP SRB-Routed Environment



The following commands show a sample configuration for Router-1 in Figure 37:

```
hostname Router-1
!
ip routing
!
! Configure the config-server database mpoa-db with configuration
! for ELANs 1 to 3
lane database mpoa-db
  name 1 server-atm-address 47.0091810000000060705BFA01.00000CA05F41.01
  name 1 local-seg-id 1000
  name 1 elan-id 100
  name 2 server-atm-address 47.0091810000000060705BFA01.00000CA05B41.01
  name 2 local-seg-id 2000
  name 2 elan-id 200
  name 3 server-atm-address 47.0091810000000060705BFA01.00000CA05B41.03
  name 3 local-seg-id 3000
  name 3 elan-id 300
!
! Define the MPOA Server (mps-1) configuration.
mpoa server config name mps-1
```

```
!
! Configure the signalling and ILMI PVCs. Also configure a config-server
! and attach the MPOA server (mps-1) to its ATM interface.
interface ATM4/0
  no ip address
  atm pvc 1 0 5 qsaal
  atm pvc 2 0 16 ilmi
  lane config auto-config-atm-address
  lane config database mpoa-db
  mpoa server name mps-1
!
! Configure a Token Ring LANE client on ELAN 1 and bind the LANE
! client to its MPOA server (mps-1). The multiring ip configuration
! is required to terminate the RIF for IP packets on the ELAN.
interface ATM4/0.1 multipoint
  ip address 1.1.1.2 255.255.255.0
  lane client mpoa server name mps-1
  lane client tokenring 1
  multiring ip
!
! Configure a Token Ring LANE client on ELAN 2 and bind the LANE
! client to its MPOA server (mps-1)
!
 interface ATM4/0.2 multipoint
   ip address 2.2.2.1 255.255.255.0
   lane client mpoa server name mps-1
   lane client tokenring 2
!
!
 router eigrp 1
   network 1.0.0.0
   network 2.0.0.0
!
end
```

The following commands show a sample configuration for Router-2 in Figure 37:

```
hostname Router-2
!
ip routing
!
! Defines the MPOA Server (mps-2) configuration.
mpoa server config name mps-2
!
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! server (mps-2) to its ATM interface.
interface ATM2/0
 no ip address
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 mpoa server name mps-2
!
! Configure a Token Ring LANE client and LANE server-bus on ELAN 2
! and bind the LANE client to its MPOA server (mps-2)
!
interface ATM2/0.1 multipoint
 ip address 2.2.2.2 255.255.255.0
 lane server-bus tokenring 2
 lane client mpoa server name mps-2
 lane client tokenring 2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA server (mps-2)
!
```

```
interface ATM2/0.3 multipoint
 ip address 3.3.3.1 255.255.255.0
 lane server-bus tokenring 3
 lane client mpoa server name mps-2
 lane client tokenring 3
!
router eigrp 1
 network 2.0.0.0
 network 3.0.0.0
!
end
```

The following commands show a sample configuration for Router-3 in Figure 37:

```
hostname Router-3
!
ip routing
!
! Define the MPOA client (mpc-2) configuration.
mpoa client config name mpc-2
!
!
! Configure the Token Ring interface
interface TokenRing1/0
 ip address 4.4.4.1 255.255.255.0
 ring-speed 16
!
! Configure the signalling and ILMI PVCs and attach the MPOA
! client to its ATM interface.
!
interface ATM2/0
 atm pvc 1 0 5 qsaal
 atm pvc 2 0 16 ilmi
 mpoa client name mpc-2
!
! Configure a Token Ring LANE client on ELAN 3 and bind the LANE
! client to its MPOA client (mpc-2).
!
interface ATM2/0.1 multipoint
 ip address 3.3.3.2 255.255.255.0
 lane client mpoa client name mpc-2
 lane client tokenring 3
!
router eigrp 1
 network 3.0.0.0
 network 4.0.0.0
!
end
```