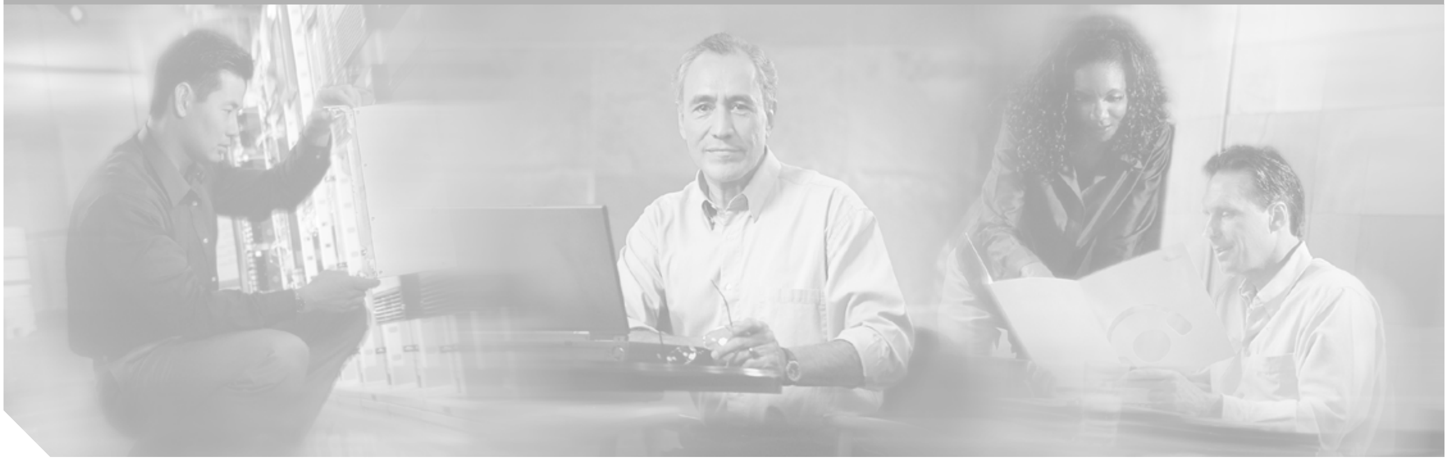


Cisco IOS Interface and Hardware Component Configuration Guide

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-7817503=
Text Part Number: 78-17503-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IOS Interface and Hardware Component Configuration Guide

CONTENTS

PART 1: LAN INTERFACES

PART 2: SERIAL INTERFACES

PART 3: VIRTUAL INTERFACES

PART 4: TUNNELS

PART 5: DIAL SHELVES

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:

- Understanding Command Modes, page xlix
- Getting Help, page l
- Using the no and default Forms of Commands, page liv
- Saving Configuration Changes, page liv
- Filtering Output from the show and more Commands, page lv
- Finding Additional Feature Support Information, page lv

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)

Command	Comment

`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)#`
	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 `Router(config-if)#`.

`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)#`
	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.

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.

Interface Configuration Overview

Use the information in this chapter to understand the types of interfaces supported on Cisco routers and access servers and to locate configuration information for various types of interfaces.

For a complete description of the interface commands used in this and other chapters that describe interface configuration, see the *Cisco IOS Interface and Hardware Component Command Reference*. To locate documentation of other commands that appear in this chapter, use the master commands list or search online.

For a list of interface types supported on Cisco routers, see the "Interface Types Supported on Cisco Routers" section on page 2.

For information about a specific type of interface, see the chapter or publication indicated in Table 3.

Table 3 Locating Information About Interface Types

For this interface type...	And these tasks...	See this chapter or publication...
Dialed interfaces	• Configuring channelized E1, channelized T1, or channelized T1 on the Cisco AS5200 • Configuring a dialer interface • Configuring an ISDN BRI, MBRI, or PRI interface • Managing Dial Shelves	*Cisco IOS Dial Technologies Configuration Guide* and *Cisco IOS Dial Technologies Command Reference.* "Managing Dial Shelves" in the *Cisco IOS Interface and Hardware Component Configuration Guide*
LAN interfaces	• Configuring Ethernet, Fast Ethernet, or Gigabit Ethernet interfaces • Configuring Fast EtherChannel • Configuring a FDDI interface • Configuring a hub interface • Configuring a Token Ring interface	"Configuring LAN Interfaces" in the *Cisco IOS Interface and Hardware Component Configuration Guide*

Table 3 Locating Information About Interface Types (continued)

For this interface type...	And these tasks...	See this chapter or publication...
Serial interfaces	• Configuring a high-speed serial interface • Configuring a synchronous serial interface • Configuring a channelized T3 interface processor • Configuring PA-E3 and PA-2E3 serial port adapters • Configuring PA-T3 and PA-2T3 serial port adapters • Configuring a packet OC-3 interface • Configuring a DPT OC-12c interface • Configuring automatic protection switching of Packet-over-SONET (POS) circuits • Configuring serial interfaces for CSU/DSU service modules • Configuring low-speed serial interfaces	"Configuring Serial Interfaces" in the *Cisco IOS Interface and Hardware Component Configuration Guide*
Virtual or logical interfaces	• Configuring a loopback interface • Configuring a null interface	"Configuring Virtual Interfaces" in the *Cisco IOS Interface and Hardware Component Configuration Guide*
Tunnel interfaces	• Configuring a tunnel interface	"Implementing Tunnels" in the *Cisco IOS Interface and Hardware Component Configuration Guide*
Cisco Mainframe Channel Connection (CMCC) adapters	• Configuring a Channel Interface Processor (CIP) • Configuring a Channel Port Adapter (CPA)	"Configuring Cisco Mainframe Channel Connection Adapters" in the *Cisco IOS Bridging and IBM Networking Configuration Guide*

Interface Types Supported on Cisco Routers

Two types of interfaces are supported: physical and virtual interfaces. The types of physical interfaces on a device depend on its interface processors or port adapters. The virtual interfaces that Cisco routers and access servers support include subinterfaces and IP tunnels.

Cisco routers and access servers support numerous types of interfaces including, but not limited, to the following:

- Asynchronous serial
- ATM
- Automatic protection switching of Packet-over-SONET
- Channelized E1
- Channelized T1
- Channelized T3
- Dialer
- Ethernet
- Fast Ethernet
- FDDI
- Fractional T1/T1
- Gigabit Ethernet
- High-Speed Serial Interface (HSSI)
- ISDN BRI
- ISDN Multiple Basic Rate Interface (MBRI)
- ISDN PRI
- Loopback
- Low-speed serial
- Null
- Packet OC-3
- OC-12c Dynamic Packet Transport (DPT)
- OC-12c Dynamic Packet Transport Interface Processor (DPTIP)
- PA-E3 and PA-2E3
- PA-T3 and PA-2T3
- Synchronous serial
- Token Ring
- Tunnel

In addition, the Cisco IOS software supports subinterfaces, see the *Cisco IOS Wide-Area Networking Configuration Guide* and the protocol chapters in the Cisco IOS software configuration guides for specific information on how to configure a subinterface for a particular protocol.

For hardware technical descriptions and information about installing interfaces, see the hardware installation and maintenance publication for your product. For command descriptions and usage information, see the *Cisco IOS Interface and Hardware Component Command Reference*.

Features for Any Interface

Use the information in this chapter to understand the types of interfaces supported on Cisco routers and access servers and to locate configuration information for various types of interfaces.

To identify the hardware platform or software image information associated with a feature, use Cisco Feature Navigator on Cisco.com to search for information about the feature.

For a complete description of the interface commands used in this and other chapters that describe interface configuration, refer to the *Cisco IOS Interface and Hardware Component Command Reference*. To locate documentation of other commands that appear in this chapter, use the master commands list or search online.

This chapter contains general information that applies to all interface types; it includes the following sections:

- Understanding Interface Configuration, page 5
- Understanding Subinterfaces, page 6
- Configuring Features Available on Any Interface, page 7
- Understanding OIR, page 11
- Understanding Fast Switching Support, page 11
- Monitoring and Maintaining the Interface, page 12

For examples of configuration commands shown in this chapter, see the "Interface Configuration Examples" section on page 27.

Understanding Interface Configuration

These general instructions apply to all interface configuration processes. Begin interface configuration in global configuration mode. To configure an interface, follow these steps:

1. Use the **configure** EXEC command at the privileged EXEC prompt to enter global configuration mode.
2. Once in the global configuration mode, start configuring the interface by using the **interface** command. Identify the interface type followed by the number of the connector or interface card. These numbers are assigned at the factory at the time of installation or when cards are added to a system and can be displayed with the **show interfaces** EXEC command. A report is provided for each interface that the device supports, as seen in the following partial sample display.

```
Router# show interfaces

Serial 0 is administratively down, line protocol is down
Hardware is MCI Serial
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Use the **show hardware** EXEC command to see a list of the system software and hardware.

To begin configuring serial interface 0, add the following line to the configuration file:

```
interface serial 0
```

Note It is not necessary to add a space between the interface type and interface number. For example, in the preceding line you can specify either *serial 0* or *serial0*. The command will work either way.

3. Follow each **interface** command with the interface configuration commands that your particular interface requires. The commands that you use define the protocols and applications that will run on the interface. The commands are collected and applied to the **interface** command until you use another **interface** command, a command that is not an interface configuration command, or you type the Ctrl-Z sequence to get out of configuration mode and return to privileged EXEC mode.
4. Once an interface is configured, you can check its status by using the EXEC **show** commands listed in the tables in the "Monitoring and Maintaining the Interface" section on page 12.

Note Configuring channelized T1 and E1 interfaces requires additional steps. When you configure channelized T1or channelized E1, you must first define the channels and the time slots that comprise the channels by using the **controller t1** and the **channel-group** controller configuration commands. Then configure the virtual serial interfaces using the **interface serial** command in global configuration mode. Refer to the *Cisco IOS Dial Technologies Configuration Guide* for instructions on configuring channelized E1 or channelized T1 interfaces.

Understanding Subinterfaces

Configuring multiple virtual interfaces, or subinterfaces, on a single physical interface allows greater flexibility and connectivity on the network. A subinterface is a mechanism that allows a single physical interface to support multiple logical interfaces or networks. That is, several logical interfaces or networks can be associated with a single hardware interface. Subinterfaces are implemented in various WAN and LAN protocols, including ATM, Frame Relay, Switched Multimegabit Data Service (SMDS), X.25, and Novell IPX (Internetwork Packet Exchange). For more information about using subinterfaces, refer to the appropriate protocol chapter.

IDB Scalability

Cisco IOS software uses interface descriptor blocks (IDBs) to store interface-specific information, such as protocols configured and timers, so that Cisco IOS device drivers can interact efficiently with various types of interfaces. IDBs are an exhaustible resource tied to the memory available on the router. Each physical interface comprises a hardware IDB and at least one software IDB, although more than one software IDB may be supported and mapped to the same physical interface.

An IDB is used for each of these types of interfaces:

- Physical
- Dialer
- Virtual
- Hidden
- Subinterface
- Tunnel
- Loopback

Hardware IDBs

The hardware IDB contains physical state information about the interface. Hardware IDBs are allocated from the fast memory pool if it exists on the platform. If there is no fast memory pool, they are allocated from process memory.

Software IDBs

The software IDB contains application-specific information for the router. New software IDBs can be allocated after system initialization to create subinterfaces and virtual interfaces such as loopback and tunnel interfaces. Software IDBs are allocated from process memory.

The number of interfaces supported depends on the platform, the cards installed in the device, and auto configuration for platform and memory configuration.

Configuring Features Available on Any Interface

The following sections describe optional tasks that you can perform on any type of interface:

Adding a Description for an Interface

You can add a description about an interface to help you remember what is attached to it. This description is meant solely as a comment to help identify what the interface is being used for. The description will appear in the output of the following commands: **show configuration**, **show system:running-config**, and **show interfaces**. When you add a description for a T1 controller interface, it will appear in the output of the **show controllers t1** and **show system:running-config** commands.

To add a description for any interface except a T1 or E1 controller interface, use the following command in interface configuration mode. To add a description for a T1 or E1 controller in a Cisco 7200 series, or Cisco 7500 series router, use the following command in controller configuration mode.

Command	Purpose
`Router(config-if)# description string`	Adds a comment to help identify an interface.

For examples of adding interface descriptions, see the section "Interface Description Examples" at the end of this chapter.

Configuring MOP

To enable Maintenance Operation Protocol (MOP) on an interface, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# mop enabled`	Enables MOP.

To enable an interface to send out periodic MOP system identification messages, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# mop sysid`	Enables MOP message support.

Controlling Interface Hold-Queue Limits

Each interface has a hold-queue limit. This limit is the number of data packets that the interface can store in its hold queue before rejecting new packets. When the interface empties one or more packets from the hold queue, it can accept new packets again. To specify the hold-queue limit of an interface, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# hold-queue length {in	out}`	Specifies the maximum number of packets allowed in the hold queue.

Setting Bandwidth

Higher-level protocols use bandwidth information to make operating decisions. For example, the Interior Gateway Routing Protocol (IGRP) uses the minimum path bandwidth to determine a routing metric. TCP adjusts initial retransmission parameters on the basis of the apparent bandwidth of the outgoing interface. To set a bandwidth value for an interface, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`bandwidth`** *`kilobits`*	Sets a bandwidth value.

The bandwidth setting is a routing parameter only; it does not affect the physical interface.

Setting Interface Delay

Higher-level protocols might use delay information to make operating decisions. For example, IGRP can use delay information to differentiate between a satellite link and a land link. To set a delay value for an interface, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`delay`** *`tens-of-microseconds`*	Sets a delay value for an interface.

Setting the delay value sets an informational parameter only; you cannot adjust the actual delay of an interface using this configuration command.

Adjusting Timers

To adjust the frequency of update messages, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`keepalive`** `[`*`seconds`*`]`	Adjusts the frequency with which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (HDLC-serial and PPP-serial links) to ensure that a network interface is alive for a specified interface.

The interval is adjustable in 1-second increments down to 1 second. An interface is declared down after three update intervals have passed without receiving a keepalive packet.

When adjusting the interval for a very low bandwidth serial interface, large packets can delay the smaller keepalive packets long enough to cause the line protocol to go down. You might need to experiment to determine the best value.

Limiting Transmit Queue Size

You can control the size of the transmit queue available to a specified interface on the Multiport Communications Interface (MCI) and Serial Communication Interface (SCI) cards. To limit the size, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# **tx-queue-limit** *number*`	Limits the size of the transmit queue.

Adjusting Maximum Packet Size or MTU Size

Each interface has a default maximum packet size or maximum transmission unit (MTU) size. This number generally defaults to 1500 bytes. On serial interfaces, the MTU size varies, but cannot be set smaller than 64 bytes. To adjust the maximum packet size or MTU size, use the following command in interface configuration mode.

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

Note The maximum MTU size that can be configured on the native Gigabit Ethernet ports on the Cisco 7200 series router is 9216. The range of configurable MTU value is from 1500 to 9216.

Caution Changing an MTU size on a Cisco 7500 series router results in resizing and reassigning buffers and resetting all interfaces. The following message is displayed:

```
%RSP-3-Restart:cbus complex.
```

Using Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ip mtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

Using the mtu Command on ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, MTU on a subinterface is equal to the default MTU (4490); if a client is configured, the default is 1500. MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

Understanding OIR

The online insertion and removal (OIR) feature allows you to remove and replace interface processors while the system is online. You can shut down the interface processor before removal and restart it after insertion without causing other software or interfaces to shut down. This feature is not available on all platforms. Refer to the appropriate platform specifications for details.

Note Do not remove or install more than one interface processor at one time. After a removal or installation, ensure that the router is functioning properly before continuing.

You do not need to notify the software that you are going to remove or install an interface processor. When the Route Processor (RP) is notified by the system that an interface processor has been removed or installed, it stops routing and scans the system for a configuration change. All interface processors are initialized, and each interface type is verified against the system configuration; then the system runs diagnostics on the new interface. There is no apparent disruption to normal operation of the device during interface processor insertion or removal.

Only an interface of a type that has been configured previously will be brought online; others require configuration. If a newly installed interface processor does not match the system configuration, the interface is left in an administratively down state until the system operator configures the system with the new interfaces.

Hardware (MAC-level) addresses for all interfaces on the Cisco 7500 series routers are stored on an EEPROM component in the RP instead of on the individual interface boards. On the Cisco 7500 series routers, an address allocator in the EEPROM contains a sequential block of 40 addresses (5 interface slots times a maximum of 8 possible ports per slot); each address is assigned to a specific slot and port address in the chassis, regardless of how the interfaces are configured. On the Cisco 7200 series, hardware addresses are stored in a midplane EEPROM that supports 1024 addresses per box.

Storage of hardware addresses in EEPROM allows interfaces to be replaced online without requiring the system to update switching tables and data structures. Regardless of the types of interfaces installed, the hardware addresses do not change unless you replace the system RP. If you do replace the RP, the hardware addresses of *all* ports change to those specified in the address allocator on the new RP.

Understanding Fast Switching Support

Switching is the process by which packets are forwarded. The Cisco IOS software supports multiple methods of switching. Cisco routers fast-switch Layer 2 Forwarding (L2F) traffic. In stack group environments in which some L2F traffic is offloaded to a powerful router, fast switching provides improved scalability.

For information about switching features, refer to the *Cisco IOS IP Switching Configuration Guide*. For documentation of commands used to configure switching features, refer to the *Cisco IOS IP Switching Command Reference*.

Monitoring and Maintaining the Interface

To monitor and maintain the interfaces, you can perform the tasks in the following sections:

- Monitoring Interface and Controller Status, page 12
- Monitoring the T1 or E1 Controller, page 14
- Monitoring and Maintaining CSU/DSU Service Modules, page 14
- Monitoring and Maintaining a Hub, page 17
- Clearing and Resetting the Interface, page 18
- Shutting Down and Restarting an Interface, page 19
- Configuring Interface Index Persistence, page 20
- Configuring Loopback Detection, page 23
- Running Interface Loopback Diagnostics, page 23
- Enabling Loopback Testing of Fractional T1/T1, page 25
- Reloading a Cisco 7500 Single Line Card, page 25

Monitoring Interface and Controller Status

Cisco IOS software contains commands that you can use at the privileged EXEC or user EXEC prompt to display information about an interface including the version of the software and the hardware, the controller status, and statistics about the interfaces. The following table lists some of the interface monitoring commands. (You can display the full list of **show** commands by using the **show ?** command at the privileged EXEC or user EXEC prompt.) These commands are fully described in the *Cisco IOS Interface and Hardware Component Command Reference*.

To display information about an interface, use the following commands in privileged EXEC or user EXEC mode, as indicated.

Command	Mode	Purpose
Router# **show async status show interfaces async**	Privileged EXEC	Displays the status of the asynchronous interface.
Router> **show compress**	User EXEC	Displays compression statistics on a serial interface.
Router# **show controllers** [**bri** | **cbus** | **fddi** | **lance** | **mci** | **serial** | **token**]	Privileged EXEC	Displays current internal status information for the interface controller cards.
Router# **show controllers cbus**	Privileged EXEC	Displays information about the Switch Processor (SP) controller on the Cisco 7500 series routers.
Router> **show controllers** [**e1** | **ethernet** | **fastethernet** | **gigabitethernet** | **fddi** | **serial** | **t1** | **token**]	User EXEC	Displays current internal status information for the interface controller cards.
Router> **show controllers** [**ethernet** | **fastethernet** | **gigabitethernet** | **fddi** | **serial** | **token**]	User EXEC	Displays current internal status information for the interface controller cards on the Cisco 7200 series and Cisco 7500 series routers.

Command	Mode	Purpose
`Router# show derived-config [interface type number]`	Privileged EXEC	Displays the composite results of all the configuration commands that apply to an interface, including commands that come from sources such as static templates, dynamic templates, dialer interfaces, and AAA per-user attributes.
`Router# show diagbus [slot]`	Privileged EXEC	Displays diagnostic information about the controller, interface processor, and port adapters associated with a specified slot of a Cisco 7200 series or Cisco 7500 series router.
`Router# show interfaces [type number] [first] [last] [accounting]`	Privileged EXEC	If accounting is configured, displays the number of packets of each protocol type that have been sent through the interface.
`Router# show interfaces [type slot/port] [accounting]`		For Cisco 7500 series routers with a Packet over SONET Interface Processor.
`Router# show interfaces [type slot/port-adapter/port] [accounting]`		For Cisco 7500 series routers with VIP or VIP2 cards.
`Router# show interfaces ctunnel interface-number`	Privileged EXEC	Displays information about an IP over CLNS tunnel.
`Router> show interfaces pos [slot/port]`	User EXEC	Displays information about Cisco 7500 series with a Packet over SONET Interface Processor.
`Router# show interfaces async [number] [accounting]`	Privileged EXEC	Displays the number of packets of each protocol type that have been sent through the asynchronous serial line.
`Router# show system:running-config`	Privileged EXEC	Displays the currently running configuration in RAM.
`Router# show rif`	Privileged EXEC	Displays the current contents of the Routing Information Field (RIF) cache.
`Router# show protocols`	Privileged EXEC	Displays the global (system-wide) and interface-specific status of any configured Level 3 protocol.
`Router# show version`	Privileged EXEC	Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.

Monitoring the T1 or E1 Controller

This section applies to channelized T1 or E1 interfaces. Because the T1 or E1 link itself is viewed as the controller, use the following commands in privileged EXEC mode to display information about activity on the T1 or E1 line.

Command	Purpose
`Router# show controllers t1`	Displays information about the T1 link.
`Router# show controllers e1`	Displays information about the E1 link.

Alarms, line conditions, and other errors are displayed. The data is updated every 10 seconds. Every 15 minutes, the cumulative data is stored and retained for 24 hours. This means at any one time, up to 96 15-minute accumulations are counted in the data display.

Monitoring and Maintaining CSU/DSU Service Modules

This section describes how to monitor and maintain service modules. Tasks involved to monitor and maintain service modules are described in these sections:

- Performing a Self-Test, page 14
- Displaying a Performance Report, page 15
- Performing Loopback Tests, page 15
- Resetting the CSU/DSU, page 17

Performing a Self-Test

To perform a self-test on the integrated channel service unit/data service unit (CSU/DSU), use the following command in privileged EXEC mode.

Command	Purpose
`Router# test service-module interface`	Performs a self-test. Specifies the interface type and number.

This command cannot be used if a DTE, line, or remote loopback is in progress. A series of tests are performed on the CSU/DSU, which include a ROM checksum test, a RAM test, an EEPROM checksum test, a flash checksum test, and a DTE loopback with an internal pattern test. This self-test is also performed at power on.

Data transmission is interrupted for 5 seconds when you issue this command. To view the output of the most recent self-test, enable the **show service-module** command.

Displaying a Performance Report

To display the performance report for an integrated CSU/DSU, use one of the following commands in privileged EXEC mode.

Command	Purpose
`Router# show service-module interface`	Displays a performance report. Choose either serial interface 1 or serial interface 0.
`Router# show service-module interface performance-statistics [interval-range]`	Displays the CSU/DSU performance statistics for the past 24 hours. This command applies only to the FT1/T1 module.

The *interval-range* value specifies the number of 15-minute intervals displayed in the report. You can choose a range from 1 to 96, where each value represents the CSU/DSU activity performed in that 15-minute interval. For example, a range of 2-3 displays the performance statistics for the intervals two and three.

Performing Loopback Tests

You can loop packets back to the network from the integrated CSU/DSU and loop packets through a local CSU/DSU to a remote CSU/DSU.

Performing Loopback Line Test

To loop data received from the line at the integrated CSU/DSU and loop packets back to the line, use the following commands in interface configuration mode.

	Command	Purpose
Step 1	`Router(config-if)# loopback line`	Performs loopback on the network at a point physically near the CSU/DSU interface.
Step 2	`Router(config-if)# loopback line payload`	Performs loopback on the network at a point physically near the interface between the CSU/DSU and the router.

Packets are looped from an incoming network transmission back into the network at a CSU or DSU loopback point.

When the **loopback line** command is configured on the 2-wire, 56-kbps CSU/DSU module or the 4-wire, 56/64-kbps CSU/DSU modules installed on a Cisco 2524 or Cisco 2525 router, the network data loops back at the CSU and the router data loops back at the DSU. If the CSU/DSU is configured for switched mode, you must have an established connection to perform a payload-line loopback. When the **loopback line payload** command is configured, the CSU/DSU module loops the data through the DSU portion of the module. Data is not looped back to the serial interface.

If you enable the **loopback line** command on the fractional T1/T1 module, the CSU/DSU performs a full-bandwidth loopback through the CSU portion of the module and data transmission through the serial interface is interrupted for the duration of the loopback. No reframing or corrections of bipolar violation errors or cyclic redundancy check (CRC) errors are performed. When you configure the **line loopback payload** command on the FT1/T1 module, the CSU/DSU performs a loopback through the DSU portion of the module. The **line loopback payload** command reframes the data link, regenerates the signal, and corrects bipolar violations and Extended Super Frame (ESF) CRC errors.

When performing a T1-line loopback with Extended Super Frame, communication over the facilities data link is interrupted but performance statistics are still updated. To show interfaces currently in loopback operation, use the **show service-module** privileged EXEC command.

Performing Loopback DTE

To loop packets back to DTE from within the local CSU/DSU, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`loopback dte`**	Loops packets to DTE.

Packets are looped from within the CSU/DSU back to the serial interface of the router. Send a test ping to see if the packets successfully looped back. To cancel the loopback test, use the **no loopback dte** command.

When using the 4-wire, 56/64-kbps CSU/DSU module, an out-of-service signal is transmitted to the remote CSU/DSU.

Performing a Remote Loopback Test Using the FT1/T1 CSU/DSU Module

The **loopback** command applies only when the remote CSU/DSU device is configured for this function. It is used for testing the data communication channels along with or without remote CSU/DSU circuitry. The loopback is usually performed at the line port, rather than the DTE port, of the remote CSU/DSU.

On the integrated FT1/T1 CSU/DSU module installed on a Cisco 2524 and Cisco 2525 router, the **loopback remote full** command sends the loopup code to the remote CSU/DSU. The remote CSU/DSU should perform a full-bandwidth loopback through the CSU portion of the module. The **loopback remote payload** command sends the loopup code on the configured time slots, while maintaining the D4-Extended Super Frame. The remote CSU/DSU performs the equivalent of a loopback line payload request. The remote CSU/DSU loops back only those time slots that are configured on the remote end. This loopback reframes the data link, regenerates the signal, and corrects bipolar violations and Extended Super Frame CRC errors. The **loopback remote smart-jack** command sends a loopup code to the remote smart jack. You cannot put the local smart jack into loopback.

To loop packets on the integrated FT1/T1 CSU/DSU module, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`loopback remote`** `{`**`full`** `|` **`payload`** `|` **`smart-jack`**`}[`**`0in1`** `|` **`1in1`** `|` **`1in2`** `|` **`1in5`** `|` **`1in8`** `|` **`3in24`** `|`**`qrw`** `|` **`user-pattern`** *`24bit-binary value`*`]`	Loops packets at a remote CSU/DSU using the fractional FT1/T1 CSU/DSU module.

Failure to loop up or initiate a remote loopback request could be caused by enabling the **no service-module t1 remote-loopback** command or having an alternate remote-loopback code configured on the remote end. When the loopback is terminated, the result of the pattern test is displayed.

Note If the FT1/T1 CSU/DSU module is configured to provide internal clocking, the module ceases to generate clocking when it is placed into loopback.

2- and 4-Wire, 56/64-kbps CSU/DSU Modules

The **loopback** command applies only when the remote CSU/DSU device is configured for this function. It is used for testing the data communication channels along with or without remote CSU/DSU circuitry. The loopback is usually performed at the line port, rather than the DTE port, of the remote CSU/DSU.

On the 2- and 4-wire, 56/64-kbps CSU/DSU modules, an active connection is required before a loopup can be initiated while in switched mode. When transmitting V.54 loopbacks, loopback is initiated for the remote device using V.54 messages. Failure to loop up or initiate a remote loopback request could be caused by enabling the **no service-module 56k remote-loopback** command.

To loop packets at the remote CSU/DSU, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# **loopback remote** [**2047** | **511** | **stress-pattern** *pattern number*]`	Loops packets at a remote CSU/DSU using the 2- and 4-wire, 56/64-kbps CSU/DSU modules.

To display loopback interfaces, use the **show interfaces loopback** EXEC command.

Resetting the CSU/DSU

To reset the CSU/DSU, use the following command in privileged EXEC mode.

Command	Purpose
`Router# **clear service-module** *interface*`	Resets the CSU/DSU. Specifies the interface type and number.

Use this command only in severe circumstances (for example, when the router is not responding to a CSU/DSU configuration command).

This command terminates all DTE and line loopbacks that are locally or remotely configured. It also interrupts data transmission through the router for up to 15 seconds. The software performs an automatic software reset in the case of two consecutive configuration failures.

The CSU/DSU module is not reset with the **clear interface** command.

Caution If you experience technical difficulties with your router and intend to contact customer support, do not use this command. The command erases the past CSU/DSU performance statistics of the router. To clear only the CSU/DSU performance statistics, issue the **clear counters** command.

Monitoring and Maintaining a Hub

To monitor and maintain a hub, you can perform the tasks in the following sections:

- Shutting Down the Hub Port, page 18
- Resetting the Hub or Clearing the Hub Counters, page 18
- Monitoring the Hub, page 18

Shutting Down the Hub Port

To shut down or disable a hub port, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)# hub ethernet number port [end-port]`	Specifies the hub number and the hub port (or range of hub ports) and enters hub configuration mode.
Step 2	`Router(config-hub)# shutdown`	Shuts down the hub port.

See the examples of shutting down a hub port in the "Hub Configuration Examples" section of the "Configuring LAN Interfaces" chapter.

Resetting the Hub or Clearing the Hub Counters

To reset the hub or clear the hub counters, use one of the following commands in user EXEC mode.

Command	Purpose
`Router> clear hub ethernet number`	Resets and reinitializes the hub hardware.
`Router> clear hub counters [ethernet number [port [end-port]]]`	Clears the hub counters displayed by the **show hub** command.

Monitoring the Hub

To display hub information, use the following command in user EXEC mode.

Command	Purpose
`Router> show hub [ethernet number [port [end-port]]]`	Displays hub statistics.

Clearing and Resetting the Interface

To clear the interface counters displayed with the **show interfaces** command, use any of the following commands in user EXEC mode.

Command	Purpose
`Router> clear counters [type number] [ethernet | serial]`	Clears the interface counters.
`Router> clear counters fastethernet number`	Clears interface counters for the Fast Ethernet NIM on the Cisco 4000 series or Cisco 4500 series routers.
`Router> clear counters [type slot/port]`	Clears interface counters for the Cisco 7200 series routers.
`Router> clear counters [type slot/port-adaptor]`	Clears interface counters for the Cisco 7500 series with VIP or VIP2 Interface Processors.

The **clear counters** command clears all the current interface counters from the interface unless the optional arguments are specified to clear only a specific interface type from a specific slot and port number.

Note The **clear counters** command will not clear counters retrieved using SNMP (Simple Network Management Protocol), but only those seen with the **show interfaces** command in user EXEC mode.

To clear and reset interfaces, use the following commands in user EXEC mode. Under normal circumstances, you do not need to clear the hardware logic on interfaces.

	Command	Purpose
Step 1	`Router>` **`clear interface`** *`type number`*	Resets the hardware logic on an interface.
Step 2	`Router>` **`clear line`** `[`*`number`*`]`	Resets the hardware logic on an asynchronous serial line.
Step 3	`Router>` **`clear rif-cache`**	Clears the entire Token Ring RIF cache.

Shutting Down and Restarting an Interface

You can disable an interface by shutting it down. Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface will not be mentioned in any routing updates. On serial interfaces, shutting down an interface causes the dedicated Token Ring (DTR) signal to be dropped. On Token Ring interfaces, shutting down an interface causes the interface to deinsert from the ring. On FDDI interfaces, shutting down an interface causes the optical bypass switch, if present, to go into bypass mode.

To shut down an interface and then restart it, use the following commands in interface configuration mode.

	Command	Purpose
Step 1	`Router(config-if)#` **`shutdown`**	Shuts down an interface.
Step 2	`Router(config-if)#` **`no shutdown`**	Enables an interface that has been disabled.

To check whether an interface is disabled, use the **show interfaces** command in user EXEC mode. An interface that has been shut down is shown as administratively down in the **show interfaces** command display. See the examples in the "Interface Shutdown Examples" section on page 28.

One reason to shut down an interface is if you want to change the electrical interface type or mode of a Cisco 7500 series port online. You replace the serial adapter cable and use software commands to restart the interface, and if necessary, reconfigure the port for the new interface. At system startup or restart, the Fast Serial Interface Processor (FSIP) polls the interfaces and determines the electrical interface type of each port (according to the type of port adapter cable attached). However, it does not necessarily poll an interface again when you change the adapter cable online. To ensure that the system recognizes the new interface type, shut down using the **shutdown** command, and enable the interface after changing the cable. Refer to your hardware documentation for more details.

Configuring Interface Index Persistence

Interface Index Persistence allows interfaces to be identified with unique values that will remain constant even when a device is rebooted. These interface identification values are used for network monitoring and management using SNMP.

One of the identifiers most commonly used in SNMP-based network management applications is the interface index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface; as far as most software is concerned, the ifIndex is the “name” of the interface.

Although there is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection increasingly depend on the maintenance of this correspondence.

IfIndex persistence means that the mapping between the ifDescr object values and the ifIndex object values (generated from the IF-MIB) will be retained across reboots.

Interface Index Persistence allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics. Relating each interface to a known entity, such as an Internet service provider (ISP), allows network management data to be more effectively utilized.

Network data is increasingly being used worldwide for usage-based billing, network planning, policy enforcement, and trend analysis. The ifIndex information is used to identify input and output interfaces for traffic flows and SNMP statistics. Inability to reliably relate each interface to a known entity, such as a customer, invalidates the data.

The interface-specific ifIndex persistence command **snmp ifindex persistence** cannot be used on subinterfaces. A command applied to an interface is automatically applied to all the subinterfaces associated with that interface.

Testing indicates that approximately 25 bytes of NVRAM storage are used by this feature per interface. There may be some boot delay exhibited on platforms with lower CPU speeds.

For more information on configuring and using ifIndex persistence, refer to the following documents:

- The “Configuring SNMP Support” chapter of the *Cisco IOS Network Management Configuration Guide* (available at Cisco.com)
- The SNMP commands in the *Cisco IOS Network Management Command Reference* (available at Cisco.com)
- *Ethernet-like Interfaces MIB and Interfaces Group MIB Enhancements* feature module, Cisco IOS Release 12.1(2)T (available at Cisco.com)

MIBs Supported for This Feature

- Interfaces MIB (IF-MIB)

Note that this feature does not change any existing MIBs or add any new MIBs.

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

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

RFC Compliance to Support This Feature

- RFC 2233, *The Interfaces Group MIB Using SMIv2*

  RFCs are available from a variety of internet sources. The primary source is the IETF’s website at http://www.ietf.org.

Interface Index Persistence Configuration Task List

The configuration tasks described in this section assume that you have configured SNMP on your routing device and that you are using SNMP to monitor network activity using the Cisco IOS command-line interface and/or a network management system (NMS) application.

See the following sections for configuration tasks for the Interface Index Persistence feature. Each task in the list is identified as required or optional.

- Enabling and Disabling IfIndex Persistence Globally, page 21 (Optional)
- Enabling and Disabling IfIndex Persistence on Specific Interfaces, page 21 (Optional)

Enabling and Disabling IfIndex Persistence Globally

IfIndex persistence is disabled by default. To globally enable ifIndex values that are maintained across reboots, use the following command in global configuration mode.

Command	Purpose
`Router(config)# snmp-server ifindex persist`	Globally enables ifIndex values that will remain constant across reboots.

To globally disable ifIndex persistence after enabling it, use the following command in global configuration mode.

Command	Purpose
`Router(config)# no snmp-server ifindex persist`	Disables global ifIndex persistence.

Note After ifIndex persistence commands have been entered, the configuration must be saved using the **copy running-config startup-config** command in EXEC mode to ensure consistent ifIndex values.

Enabling and Disabling IfIndex Persistence on Specific Interfaces

To enable ifIndex persistence on a specific interface only, use the following commands, beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)# interface type slot/port`	Enters interface configuration mode for the specified interface. Note that the syntax of the interface command will vary depending on the platform that you are using.
Step 2	`Router(config-if)# snmp ifindex persist`	Enables an ifIndex value that is constant across reboots on the specified interface.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.

To disable ifIndex persistence on a specific interface only, use the following commands, beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# **interface** *type slot*/*port*	Enters interface configuration mode for the specified interface. Note that the syntax of the interface command will vary depending on the platform that you are using.
Step 2	Router(config-if)# **no snmp ifindex persist**	Disables an ifIndex value that is constant across reboots on the specified interface.
Step 3	Router(config-if)# **exit**	Exits interface configuration mode.

To clear the interface-specific ifIndex persistence setting and configure the interface to use the global configuration setting, use the following commands, beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# **interface** *type slot*/*port*	Enters interface configuration mode for the specified interface. Note that the syntax of the interface command will vary depending on the platform that you are using.
Step 2	Router(config-if)# **snmp ifindex clear**	Clears any interface-specific ifIndex persistence configuration for the specified interface. The ifIndex setting (enabled or disabled) will match the global configuration setting.
Step 3	Router(config-if)# **exit**	Exits interface configuration mode.

When you clear the interface-specific setting, only the global ifIndex persistence setting will apply to the interface. Regardless of whether the specific interface has ifIndex persistence enabled or disabled, the ifIndex persistence setting will default to the global setting after you issue the **snmp ifindex clear** command.

For example, assume that you enabled ifIndex persistence on Ethernet interface 0/1, and then globally enabled ifIndex persistence. Using the **snmp ifindex clear** command in interface configuration mode for Ethernet interface 0/1 would leave that interface with ifIndex enabled, because the global setting is to have ifIndex persistence enabled.

Likewise, if you disabled ifIndex persistence for Ethernet interface 0/1, globally enabled ifIndex persistence, and then issued the **snmp ifindex clear** command on that interface, ifIndex would be enabled (according to the global setting) on that interface.

Tip Use the **snmp ifindex clear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears any ifIndex configuration commands previously entered for that specific interface.

To verify that ifIndex commands have been configured, use the **more system:running-config** command.

Configuring Loopback Detection

When an interface has a backup interface configured, it is often desirable that the backup interface be enabled when the primary interface is either down or in loopback. By default, the backup is only enabled if the primary interface is down. By using the **down-when-looped** command, the backup interface will also be enabled if the primary interface is in loopback. To achieve this condition, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# down-when-looped`	Configures an interface to tell the system it is down when loopback is detected.

If testing an interface using the loopback command, you should not have loopback detection configured, or packets will not be transmitted out the interface that is being tested.

Running Interface Loopback Diagnostics

You can use a loopback test on lines to detect and distinguish equipment malfunctions between line and modem or CSU/DSU problems on the network server. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem. The DSU might have similar loopback functions that you can use to isolate the problem if the interface loopback test passes. If the device does not support local loopback, this function will have no effect.

You can specify hardware loopback tests on the Ethernet and synchronous serial interfaces and on all Token Ring interfaces that are attached to CSU/DSUs and that support the local loopback signal. The CSU/DSU acts as a DCE device; the router or access server acts as a DTE device. The local loopback test generates a CSU loop—a signal that goes through the CSU/DSU to the line, then back through the CSU/DSU to the router or access server. The **ping** command can also be useful during loopback operation.

The loopback tests are described in the following sections:

- High-Speed Serial Interface (HSSI), including the High-Speed Communications Interface (HSCI) card ribbon cable
- Cisco Multiport Communications Interface (MCI) and Cisco Serial Communication Interface (SCI) synchronous serial interfaces
- MCI and Cisco Multiport Ethernet Controller (MEC) Ethernet interfaces (an Ethernet loopback server is also provided on the Ethernet interfaces.)
- Ethernet loopback server
- Channelized E1 interfaces (local loopback only)
- Channelized T1 interfaces (local and remote loopback)
- Fractional T1/T1 interfaces
- Token Ring interfaces
- Channelized E1 controller and interface (local loopback only)
- Channelized T1 controller and interface (local and remote loopback)
- Troubleshooting channelized E1 and channelized T1

The following sections describe each test.

Note Loopback does not work on an X.21 DTE because the X.21 interface definition does not include a loopback definition.

Enabling Loopback Testing on the HSSI

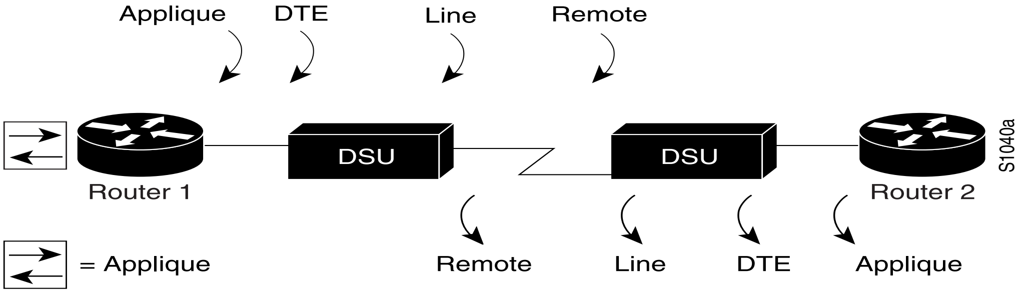
The HSSI allows you to perform the tasks described in these sections:

- Enabling a Loopback Test to the DTE, page 24
- Enabling a Loopback Test Through the CSU/DSU, page 24
- Enabling a Loopback Test over a Remote DS-3 Link, page 25

These tests apply only when the device supports them and are used to check the data communication channels. The tests are usually performed at the line port rather than at the DTE port of the remote CSU/DSU.

The internal loopback concepts are illustrated in Figure 1.

Figure 1 HSSI Loopback Testing



Enabling a Loopback Test to the DTE

You can loop packets to DTE within the CSU/DSU at the DTE interface, when the device supports this function. Doing so is useful for testing the DTE-to-DCE cable. To loop the packets to DTE, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# loopback dte`	Loops packets to DTE internally.

Enabling a Loopback Test Through the CSU/DSU

You can loop packets completely through the CSU/DSU to configure a CSU loop, when the device supports this feature. Doing so is useful for testing the DCE device (CSU/DSU) itself. To configure a CSU loop, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# loopback line`	Loops packets completely through the CSU/DSU.

Enabling a Loopback Test over a Remote DS-3 Link

You can loop packets through the CSU/DSU, over the digital signal level 3 (DS-3) link, and to the remote CSU/DSU and back. To do this, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# loopback remote`	Loops packets through the CSU/DSU to a remote CSU/DSU over the DS-3 link.

This command applies only when the device supports the remote function. It is used for testing the data communication channels. The loopback usually is performed at the line port, rather than the DTE port, of the remote CSU/DSU.

Configuring the Ethernet Loopback Server

The router software provides an Ethernet loopback server that supports Digital Equipment Corporation (Digital), Intel, and Xerox systems specified by the "blue book," a joint specification written by Digital, Intel, and Xerox that defines the Ethernet protocol. The loopback server responds to forward data loopback messages sent either to the MAC address of the server or to the broadcast address. Currently, the Ethernet loopback server does not respond to the loopback assistance multicast address.

Use the Ethernet loopback server to test communications between your internetworking products and Digital systems that do not support the IP **ping** command, such as DECnet-only VMS systems.

To originate a loop test on your VMS system with a Cisco server, use the Digital Network Control Program (NCP) **loop circuit** command. For more information about the **loop circuit** command, consult the DECnet VAX documentation. Cisco network servers support all options that can be specified by the VMS hosts.

Enabling Loopback on Token Ring Cards

To place all Token Ring interface cards into loopback mode, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# loopback`	Enables loopback and verifies that the Token Ring interface receives back every packet it sends.

Enabling Loopback Testing of Fractional T1/T1

For information, see the "Performing Loopback Tests" section on page 15.

Reloading a Cisco 7500 Single Line Card

The Cisco IOS software allows users to correct a line card failure on a Cisco 7500 series router by reloading the failed line card without reloading any other line cards on the network backplane. During the single line card reload process, all physical lines and routing protocols on the other line cards of the network backplane remain active.

The Cisco 7500 Single Line Card Reload feature works on all route switch processor (RSP) images for all Cisco IOS releases that support the Cisco 7500 Single Line Card Reload feature.

Improved Line Card Recovery Time

Use this feature to correct a line card hardware failure when the Cisco 7500 Single Line Card Reload feature is enabled. The entire system, which now only reloads one line card instead of every line card, also experiences a dramatic improvement in recovery time.

Network Traffic Flow Improvements

Because the Cisco 7500 Single Line Card Reload feature only reloads the line card with the hardware failure rather than all of the line cards on the Cisco 7500 network backplane, the active line cards can continue to forward network traffic.

Configuring Cisco 7500 Single Line Card Reloading

To enable the Cisco 7500 Single Line Card Reloading feature on the Cisco 7500 series router, use the **service single-slot-reload-enable** command in global configuration mode.

Command	Purpose
`Router(config)#` **`service single-slot-reload-enable`**	Enables single line card reloading for all of the line cards in the Cisco 7500 series router.

Disabling Cisco 7500 Single Line Card Reloading

The Cisco 7500 Single Line Card Reloading feature is disabled by default. Therefore, the process for disabling the Cisco 7500 Single Line Card Reloading feature is only necessary if the Cisco 7500 Single Line Card Reloading feature has been enabled by the user on the Cisco 7500 series router.

To disable the Cisco 7500 Single Line Card feature, enter the **no service single-slot-reload-enable** command global configuration mode on the Cisco 7500 series router.

Command	Purpose
`Router(config)#` **`no service single-slot-reload-enable`**	Disables single line card reloading for all line cards in the Cisco 7500 series router.

Verifying Cisco 7500 Single Line Card Reloading

Use the **show running-config** command to verify that single line card reloading has been successfully enabled on the Cisco 7500 series router. If the “service single-slot-reload-enable” line appears in the command output, Cisco 7500 Single Line Card Reloading is enabled. If this line does not appear in the command output, Cisco 7500 Single Line Card Reloading is disabled.

Use the **show diag** command to display hardware information on line cards, including the history of line card reloads.

Troubleshooting Tips

The **debug oir** command is used to debug the online insertion and removal (OIR) feature (which is also known as hot-swapping or power-on servicing). The **debug oir** command is often useful in debugging problems related to OIR, including single line card reloading.

Interface Configuration Examples

This section includes the following examples to illustrate configuration tasks described in this chapter:

- Interface Enablement Configuration Examples, page 27
- Interface Description Examples, page 27
- Interface Shutdown Examples, page 28
- Interface Index Persistence Examples, page 28
- Cisco 7500 Line Card Reload Examples, page 29

Interface Enablement Configuration Examples

The following example illustrates how to begin interface configuration on a serial interface. It assigns PPP encapsulation to serial interface 0.

```
interface serial 0
 encapsulation ppp
```

The same example on a Cisco 7500 series routers requires the following commands:

```
interface serial 1/0
 encapsulation ppp
```

Specific IP Addresses Configuration for an Interface Example

This example shows how to configure the access server so that it will use the default address pool on all interfaces except interface 7, on which it will use an address pool called lass:

```
ip address-pool local
ip local-pool lass 172.30.0.1
 async interface
 interface 7
 peer default ip address lass
```

Interface Description Examples

The following example illustrates how to add a description about an interface that will appear in configuration files and monitoring command displays:

```
interface ethernet 0
 description First Ethernet in network 1
 ip address 172.18.15.78 255.255.255.0
```

The following example for a Cisco 7500 series routers describes an administration network attached to the Ethernet processor in slot 2, port 4:

```
interface ethernet 2/4
 description 2nd floor administration net
```

Interface Shutdown Examples

The following example turns off the Ethernet interface in slot 2 at port 4:

```
interface ethernet 2/4
 shutdown
```

The following example restarts the interface:

```
interface ethernet 2/4
 no shutdown
```

The following example shuts down a Token Ring interface:

```
interface tokenring 0
 shutdown
```

The following example shuts down a T1 circuit number 23 that is running on a Cisco 7500 series router:

```
interface serial 4/0:23
 shutdown
```

The following example shuts down the entire T1 line physically connected to a Cisco 7500 series router:

```
controller t1 4/0
 shutdown
```

Interface Index Persistence Examples

This section provides the following configuration examples:

- Enabling IfIndex Persistence on All Interfaces Example, page 28
- Enabling IfIndex Persistence on a Specific Interface Example, page 28
- Disabling IfIndex Persistence on a Specific Interface Example, page 29
- Clearing IfIndex Persistence Configuration from a Specific Interface Example, page 29

Enabling IfIndex Persistence on All Interfaces Example

In the following example, ifIndex persistence is enabled for all interfaces:

```
snmp-server ifindex persist
```

Enabling IfIndex Persistence on a Specific Interface Example

In the following example, ifIndex persistence is enabled for Ethernet interface 0/1 only:

```
interface ethernet 0/1
 snmp ifindex persist
 exit
```

Disabling IfIndex Persistence on a Specific Interface Example

In the following example, ifIndex persistence is disabled for Ethernet interface 0/1 only:

```
interface ethernet 0/1
 no snmp ifindex persist
 exit
```

Clearing IfIndex Persistence Configuration from a Specific Interface Example

In the following example, any previous setting for ifIndex persistence on Ethernet interface 0/1 is removed from the configuration. If ifIndex persistence is globally enabled, ifIndex persistence will be enabled for Ethernet interface 0/1. If ifIndex persistence is globally disabled, ifIndex persistence will be disabled for Ethernet interface 0/1.

```
interface ethernet 0/1
 snmp ifindex clear
 exit
```

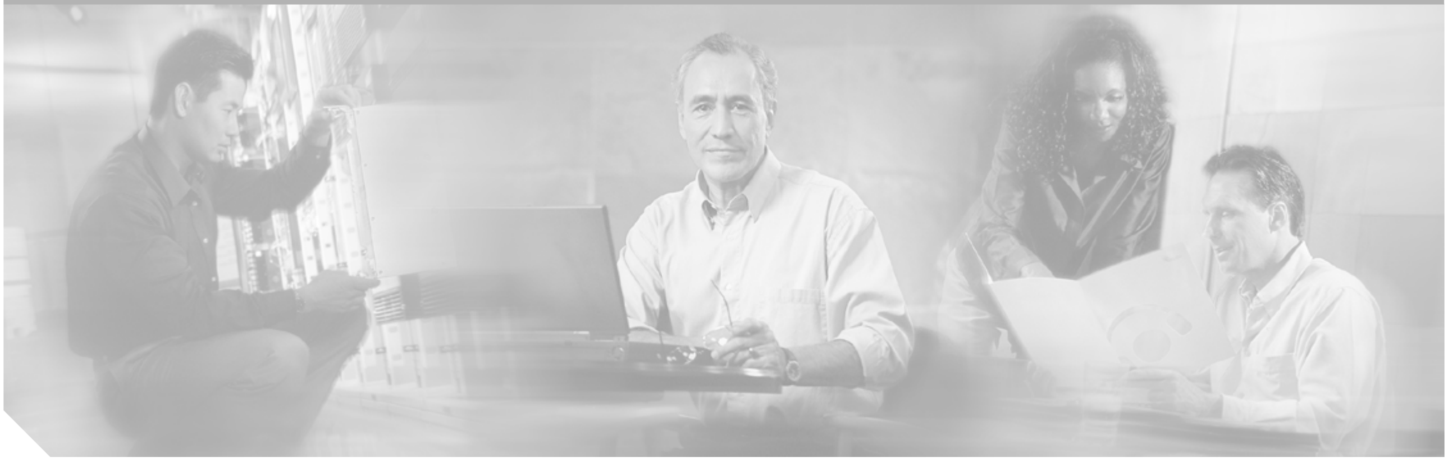
Cisco 7500 Line Card Reload Examples

In the following example, single line card reloading is enabled for all lines cards in the Cisco 7500 series router:

```
service single-slot-reload-enable
```

In the following example, single line card reloading is disabled for all line cards in the Cisco 7500 series router:

```
no service single-slot-reload-enable
```



Part 1: LAN Interfaces

Configuring LAN Interfaces

Use the information in this chapter to configure LAN interfaces supported on Cisco routers and access servers.

To identify the hardware platform or software image information associated with a feature, use Cisco Feature Navigator on Cisco.com to search for information about the feature.

This chapter describes the processes for configuring LAN interfaces and includes the following sections:

For examples of configuration tasks, see the "LAN Interface Configuration Examples" section on page 66.

For hardware technical descriptions and information about installing interfaces, refer to the hardware installation and configuration publication for your product. For a complete description of the LAN interface commands used in this chapter, refer to the *Cisco IOS Interface and Hardware Component Command Reference*. To locate documentation of other commands that appear in this chapter, use the master commands list or search online.

Configuring Ethernet, Fast Ethernet, or Gigabit Ethernet Interfaces

Cisco supports 10-Mbps Ethernet, 100-Mbps Fast Ethernet, and 1000-Mbps Gigabit Ethernet. Support for the 10-Mbps, 100-Mbps, and 1000-Mbps Ethernet interface is supplied on various Ethernet network interface cards or systems.

Fast Ethernet NP-1FE Module Benefits

- VLAN routing—VLAN support enables network managers to group users logically rather than by physical location. The high performance of the underlying Cisco 4700, combined with the feature-rich NP-1FE, makes it an ideal combination for a low-density, higher-performance application such as inter-VLAN routing.

- High-speed interconnections—The Fast Ethernet interface enables network managers to implement Fast-Ethernet routing solutions for optimal cost and performance across a wide range of applications, including campus or enterprise backbones and data centers. It is also a low-cost way to provide Fast-Ethernet access to traditional low-speed WAN services.
- Local area network aggregation—The Cisco 4500 or the Cisco 4700 series routers can support as many as 12 Ethernet, 4 Token Ring, or 1 FDDI segment. ISDN interfaces are also supported.

  With the Catalyst 3000 or Catalyst 5000 system, the Fast Ethernet processor can be used to aggregate up to twelve 10-Mbps LANs and give them high-speed access to such Layer 3 routing services as providing firewalls and maintaining access lists.

Cisco 7200 Series Routers with Fast Ethernet and Gigabit Ethernet

Cisco 7200 series routers support an I/O controller with an RJ-45 interface for Fast Ethernet support and an I/O controller with both RJ-45 and GBIC interfaces for Gigabit Ethernet support.

The Cisco 7200-I/O-GE+E is an Input/Output controller that provides one Gigabit Ethernet and one Ethernet port. It is equipped with a GBIC receptacle for 1000 Mbps operation and an RJ-45 receptacle for 10-Mbps operation.

The Cisco 7200-I/O-2FE/E is an I/O controller that provides two autosensing Fast Ethernet ports and is equipped with two RJ-45 receptacles for 10/100 Mbps operation.

You can configure the Fast Ethernet port for use at 100-Mbps full-duplex or half-duplex operation (half duplex is the default). The Fast Ethernet port is equipped with either a single MII receptacle or an MII receptacle and an RJ-45 receptacle. To support this new feature, the **media-type** interface command has been modified. The **media-type** command now supports two options:

- **100BASE-X**—Specifies an RJ-45 100BASE-X physical connection.
- **mii**—Specifies a media-independent interface.

The Gigabit Ethernet interface on the Cisco 7200-I/O-GE+E operates at full duplex and cannot be configured for half-duplex mode.

Second-generation Fast Ethernet Interface Processors (FEIP2-DSW-2TX and FEIP2-DSW-2FX) are available on Cisco 7500 series routers and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). The FEIP2-DSW is a dual-port, fixed-configuration interface processor that provides two 100-Mbps Fast Ethernet (FE) interfaces. Each interface on the FEIP2-DSW supports both half-duplex and full-duplex.

Refer to the *Cisco Product Catalog* for specific platform and hardware compatibility information.

Use the **show interfaces**, **show controllers mci**, and **show controllers cbus** EXEC commands to display the Ethernet port numbers. These commands provide a report for each interface supported by the router or access server.

Use the **show interfaces fastethernet** command to display interface statistics, and use the **show controllers fastethernet** to display information about the Fast Ethernet controller chip. The output shows statistics, including information about initialization block information, transmit ring, receive ring, and errors.

Use the **show interfaces gigabitethernet** command to display interface statistics, and use the **show controllers gigabitethernet** to display the information about the Gigabit Ethernet controller chip. The output shows statistics, including information about initialization block information, transmit ring, receive ring, and errors.

For information on how to configure Fast EtherChannel, see the tasks listed in the "Configuring Fast EtherChannel" section on page 48.

Ethernet, Fast Ethernet, and Gigabit Ethernet Interface Configuration Task List

To configure features on an Ethernet, Fast Ethernet, or Gigabit Ethernet interface, perform the tasks in the following sections:

- Specifying an Ethernet, Fast Ethernet, or Gigabit Ethernet Interface, page 35 (Required)
- Specifying an Ethernet Encapsulation Method, page 35 (Optional)
- Specifying Full-Duplex Operation, page 36 (Optional)
- Specifying the Media and Connector Type, page 37 (Optional)
- Extending the 10BASE-T Capability, page 37 (Optional)
- Configuring Fast Ethernet 100BASE-T, page 37 (Optional)
- Configuring PA-12E/2FE Port Adapters, page 39 (Optional)
- Configuring the 100VG-AnyLAN Port Adapter, page 44 (Optional)

Specifying an Ethernet, Fast Ethernet, or Gigabit Ethernet Interface

To specify an Ethernet interface and enter interface configuration mode, use one of the following commands in global configuration mode.

Command or Action	Purpose
`Router(config)#` **`interface ethernet`** *`number`*	Enters interface configuration mode.
`Router(config)#` **`interface ethernet`** *`slot/port`*	Enters interface configuration mode for the Cisco 7200 and Cisco 7500 series routers.
`Router(config)#` **`interface ethernet`** *`slot/port-adapter/port`*	Enters interface configuration mode for Cisco 7500 series routers.
`Router(config)#` **`interface fastethernet`** *`number`*	Enters interface configuration mode for the Cisco 4000 series with a Fast Ethernet NIM installed.
`Router(config)#` **`interface fastethernet`** *`slot/port`*	Specifies a Fast Ethernet interface and enters interface configuration mode on the Cisco 7200 series routers.
`Router(config)#` **`interface fastethernet`** *`slot/port-adapter/port`*	Specifies a Fast Ethernet interface and enters interface configuration mode on the Cisco 7500 series routers.
`Router(config)#` **`interface gigabitethernet`** *`slot/port`*	Specifies a Gigabit Ethernet interface and enters interface configuration mode on the Cisco 7200 series routers.

To display the Fast Ethernet slots and ports, use the **show interfaces fastethernet** command. The Fast Ethernet network interface module (NIM) and the Fast Ethernet Interface Processor (FEIP) default to half-duplex mode.

Specifying an Ethernet Encapsulation Method

Currently, there are three common Ethernet encapsulation methods:

- The standard Advanced Research Projects Agency (ARPA) Ethernet Version 2.0 encapsulation, which uses a 16-bit protocol type code (the default encapsulation method).

- Service access point (SAP) IEEE 802.3 encapsulation, in which the type code becomes the frame length for the IEEE 802.2 LLC encapsulation (destination and source Service Access Points, and a control byte).
- The SNAP method, as specified in RFC 1042, *Standard for the Transmission of IP Datagrams Over IEEE 802 Networks*, which allows Ethernet protocols to run on IEEE 802.2 media.

The encapsulation method that you use depends upon the routing protocol that you are using, the type of Ethernet media connected to the router or access server, and the routing or bridging application that you configure.

To establish Ethernet encapsulation of IP packets, use one of the following commands in interface configuration mode.

Command or Action	Purpose
`Router(config-if)#` **`encapsulation arpa`**	Selects ARPA Ethernet encapsulation.
`Router(config-if)#` **`encapsulation sap`**	Selects SAP Ethernet encapsulation.
`Router(config-if)#` **`encapsulation snap`**	Selects SNAP Ethernet encapsulation.

For an example of selecting Ethernet encapsulation for IP, see the "Ethernet Encapsulation Enablement Example" section on page 66.

Specifying Full-Duplex Operation

The default is half-duplex mode on the FEIP2-DSW-2FX. To enable full-duplex mode on the FEIP2-DSW-2FX (for a maximum aggregate bandwidth of 200 Mbps), use either of the following commands in interface configuration mode.

Command or Action	Purpose

`Router(config-if)#` **`full-duplex`**
or
`Router(config-if)#` **`no half-duplex`**
	Enables full-duplex on the Fast Ethernet interface of the FEIP2-DSW-2FX.

For an example of enabling full-duplex mode on Fast Ethernet, see the "Full-Duplex Enablement Operation Example" section on page 66.

Caution To prevent system problems, do not configure both FEIP2-DSW-2FX interfaces for full-duplex operation at the same time.

The FEIP2-DSW-2TX supports half-duplex only and should not be configured for full-duplex.

Specifying the Media and Connector Type

You can specify that the Ethernet network interface module (NIM) on the Cisco 4000 series routers use either the default of an attachment unit interface (AUI) and a 15-pin connector, or 10BASE-T and an RJ-45 connector. To do so, use one of the following commands in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# media-type aui`	Selects a 15-pin Ethernet connector.
`Router(config-if)# media-type 10baset`	Selects an RJ-45 Ethernet connector.

The default media connector type is an RJ-45 or SC (fiber-optic) connector. You can specify that the interface uses either an MII connector, or an RJ-45 or SC (fiber-optic) connector (this is the default). To do so, use one of the following commands in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# media-type mii`	Selects an MII Ethernet connector.
`Router(config-if)# media-type 100basex`	Selects an RJ-45 Ethernet connector for the FEIP2-DSW-2TX or an SC connector for the FEIP2-DSW-2FX.

Note When using the I/O controller that is equipped with an MII receptacle and an RJ-45 receptacle, only one receptacle can be configured for use at a time.

Extending the 10BASE-T Capability

On a Cisco 4000 series or Cisco 4500 series routers, you can extend the twisted-pair 10BASE-T capability beyond the standard 100 meters by reducing the *squelch* (signal cutoff time). This feature applies only to the LANCE controller 10BASE-T interfaces. LANCE is the AMD controller chip for the Cisco 4000 and Cisco 4500 Ethernet interface and does not apply to the Fast Ethernet interface.

To reduce squelch, use the first command in the following table in interface configuration mode. You can later restore the squelch by using the second command.

Command or Action	Purpose
`Router(config-if)# squelch reduced`	Reduces the squelch.
`Router(config-if)# squelch normal`	Returns squelch to normal.

Configuring Fast Ethernet 100BASE-T

You must configure the Fast Ethernet 100BASE-T interface on a Cisco AS5300 so that it can be recognized as a device on the Ethernet LAN. The Fast Ethernet interface supports 10- and 100-Mbps speeds with the 10BASE-T and 100BASE-T routers, hubs, and switches.

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

	Command or Action	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# interface fastethernet number`	Enters Fast Ethernet interface configuration mode.
Step 3	`Router(config-if)# ip address address subnet-mask`	Assigns an IP address and subnet mask to the interface.
Step 4	`Router(config-if)# speed {10 | 100 | auto}`	Assigns a speed to the interface. The default is 100 Mbps.[1] For relationship between duplex and speed command options, see Table 4.
Step 5	`Router(config-if)# duplex {full | half | auto}`	Sets up the duplex configuration on the Fast Ethernet interface. The default is half duplex.[1] For relationship between duplex and speed command options, see Table 4.

[1] The **auto** option automatically negotiates the speed on the basis of the speed and the peer router, hub, or switch media.

To use the autonegotiation capability (that is, to detect speed and duplex modes automatically), you must set both **speed** and **duplex** command to **auto**. Setting the **speed** command to **auto** negotiates speed only, and setting **duplex** command to **auto** negotiates duplex only. Table 4 describes the performance of the access server for different combinations of the **duplex** and **speed** command options. The specified **duplex** command option plus the specified **speed** command option produces the resulting system action.

Table 4 Relationship Between duplex and speed Command Options

duplex Command	speed Command	Resulting System Actions
`Router(config-if)# duplex auto`	`speed auto`	Autonegotiates both speed and duplex modes.
`Router(config-if)# duplex auto`	`speed 10 or speed 100`	Autonegotiates both speed and duplex modes.

`Router(config-if)# duplex half`
or
`Router(config-if)# duplex full`
	`speed auto`	Autonegotiates both speed and duplex modes.

`Router(config-if)# duplex half`	`speed 10`	Forces 10 Mbps and half duplex.
`Router(config-if)# duplex full`	`speed 10`	Forces 10 Mbps and full duplex.
`Router(config-if)# duplex half`	`speed 100`	Forces 100 Mbps and half duplex.
`Router(config-if)# duplex full`	`speed 100`	Forces 100 Mbps and full duplex.

Configuring PA-12E/2FE Port Adapters

The PA-12E/2FE Ethernet switch port adapter provides Cisco 7200 series routers with up to twelve 10-Mbps and two 10/100-Mbps switched Ethernet (10BASE-T) and Fast Ethernet (100BASE-TX) interfaces for an aggregate bandwidth of 435 Mbps, full-duplex. The PA-12E/2FE port adapter supports the Ethernet, IEEE 802.3, and IEEE 802.3u specifications for 10-Mbps and 100-Mbps transmission over unshielded twisted pair (UTP) cables.

The PA-12E/2FE port adapter offloads Layer 2 switching from the host CPU by using store-and-forward or cut-through switching technology between interfaces within the same virtual LAN (VLAN) on the PA-12E/2FE port adapter. The PA-12E/2FE port adapter supports up to four VLANs (bridge groups).

Note The PA-12E/2FE port adapter is a dual-width port adapter, which means it occupies two horizontally aligned port adapter slots when installed in a Cisco 7200 series router. (Single-width port adapters occupy individual port adapter slots in a Cisco 7200 series router.)

All interfaces on the PA-12E/2FE port adapter support autosensing and autonegotiation of the proper transmission mode (half-duplex or full-duplex) with an attached device. The first two PA-12E/2FE interfaces (port 0 and port 1) also support autosensing and autonegotiation of the proper connection speed (10 Mbps or 100 Mbps) with an attached device. If an attached device does not support autosensing and autonegotiation of the proper transmission mode, the PA-12E/2FE interfaces attached to the device automatically enter half-duplex mode. Use the **show system:running-config** command to determine if a PA-12E/2FE interface is autosensing and autonegotiating the proper transmission mode with an attached device. Use the **full-duplex** and the **half-duplex** commands to change the transmission mode of a PA-12E/2FE interface. After changing the transmission mode, use the **show interfaces** command to verify the transmission mode of the interface.

Note If you use the **full-duplex** and the **half-duplex** commands to change the transmission mode of the first two PA-12E/2FE interfaces (port 0 and port 1), the transmission speed of the two PA-12E/2FE interfaces automatically defaults to 100-Mbps. The first two PA-12E/2FE interfaces operate only at 10 Mbps when the interfaces are autosensing and autonegotiating the proper connection speed (10 Mbps or 100 Mbps) with an attached device.

To configure the PA-12E/2FE port adapter, perform the tasks in the following sections. Each task in the list is identified as either required or optional.

- Configuring the PA-12E/2FE Port Adapter, page 40 (Required)
- Monitoring and Maintaining the PA-12E/2FE Port Adapter, page 41 (Optional)
- Configuring Bridge Groups Using the 12E/2FE VLAN Configuration WebTool, page 42 (Optional)

Note If you plan to use a PA-12E/2FE interface to boot from a network (using TFTP), ensure that the interface is configured for a loop-free environment, that an IP address is configured for the interface's bridge-group virtual interface, and that system boot image 11.2(10)P is installed on your router (use the **show version** command to view the system boot image of your router). Then, *before* booting from the network server, use the **bridge-group** *bridge-group number* **spanning-disabled** command to disable the Spanning Tree Protocol configured on the interface to keep the TFTP server from timing out and closing the session. For detailed information about booting from a network using TFTP, loading a system image from a network server, and configuring the Spanning Tree Protocol on your Cisco 7200 series router, refer to the *PA-12E/2FE Ethernet Switch Port Adapter* book that accompanies the hardware and to the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

For information on other commands that can be used to configure a PA-12E/2FE port adapter, refer to the *Cisco IOS Interface and Hardware Component Command Reference*. For information on bridging, refer to the "Configuring Transparent Bridging" chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

For PA-12E/2FE port adapter configuration examples, see the "PA-12E/2FE Port Configuration Examples" section on page 67.

Configuring the PA-12E/2FE Port Adapter

This section provides instructions for a basic configuration. You might also need to enter other configuration commands depending on the requirements for your system configuration and the protocols that you plan to route on the interface. For complete descriptions of configuration commands and the configuration options available, refer to the other configuration guides and command references in the Cisco IOS documentation set.

To configure the interfaces on the PA-12E/2FE port adapter, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	`Router(config)#` **`bridge`** *`bridge-group`* **`protocol ieee`**	Specifies the type of Spanning Tree Protocol. The PA-12E/2FE port adapter supports DEC and IEEE Spanning Tree Protocols; however, we recommend using the IEEE protocol when configuring bridge groups.

Step 2	`Router(config)#` **`interface fastethernet`** *`slot/port`*
	(ports 0 and 1)
	`Router(config)#` **`interface ethernet`** *`slot/port`*
	(ports 2 through 13)
		Enters interface configuration mode for the interface that you want to configure.

Step 3	`Router(config-if)#` **`bridge-group`** *`bridge-group`*	Assigns a bridge group to the interface.
Step 4	`Router(config-if)#` **`cut-through`** `[`**`receive`** `|` **`transmit`**`]`	(Optional) Configures the interface for cut-through switching technology. The default is store-and-forward (that is, no cut-through).
Step 5	`Router(config-if)#` **`full-duplex`**	(Optional) Configures the transmission mode for full-duplex, if an attached device does not support autosensing or autonegotiation. The default is half-duplex.
Step 6	`Router(config-if)#` **`no shutdown`**	Restarts the interface.
Step 7	`Router(config-if)#` **`exit`**	Returns to global configuration mode.
Step 8	Repeat Steps 1 through 7 for each interface.	—
Step 9	`Router#` **`copy system:running-config nvram:startup-config`**	Saves the new configuration to memory.

To enable integrated routing and bridging on the bridge groups, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	`Router(config)# bridge irb`	Enables integrated routing and bridging.
Step 2	`Router(config)# interface bvi bridge-group`	Enables a virtual interface on a bridge group.
Step 3	`Router(config-if)# ip address ip-address mask`	Assigns an IP address and subnet mask to the bridge-group virtual interface.
Step 4	`Router(config-if)# no shutdown`	Restarts the interface.
Step 5	`Router(config-if)# exit`	Returns to global configuration mode.
Step 6	Repeat Steps 1 through 5 for each bridge group.	—
Step 7	`Router(config)# bridge bridge-group route protocol`	Specifies the protocol for each bridge group.
Step 8	`Router(config)# exit`	Exits global configuration mode.
Step 9	`Router# copy system:running-config nvram:startup-config`	Saves the new configuration to memory.

Monitoring and Maintaining the PA-12E/2FE Port Adapter

After configuring the new interface, you can display its status and verify other information. To display information about the PA-12E/2FE port adapter, use the following commands in EXEC mode.

Command or Action	Purpose
`Router# show version`	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot image.
`Router# show controllers`	Displays all current port adapters and their interfaces

`Router# show interfaces fastethernet slot/port`
(ports 0 and 1)
or
`Router# show interfaces ethernet slot/port`
(ports 2 through 13)
	Displays the interfaces so that you can verify that they have the correct slot number and that the interface and line protocol are in the correct state.

`Router# show bridge group`	Displays all bridge groups and their interfaces.

`Router# show interfaces fastethernet slot/port irb`
(ports 0 and 1)
or
`Router# show interfaces ethernet slot/port irb`
(ports 2 through 13)
	Displays the routed protocol so you can verify that it is configured correctly for each interface.

Command or Action	Purpose
`Router# show protocols`	Displays the protocols configured for the entire system and specific interfaces.

`Router# show pas eswitch addresses fastethernet slot/port`
(ports 0 and 1)
or
`Router# show pas eswitch addresses ethernet slot/port`
(ports 2 through 13)
	Displays the Layer 2 learned addresses for each interface.

`Router# more system:running-config`	Displays the running configuration file.
`Router# more nvram:startup-config`	Displays the configuration stored in NVRAM.

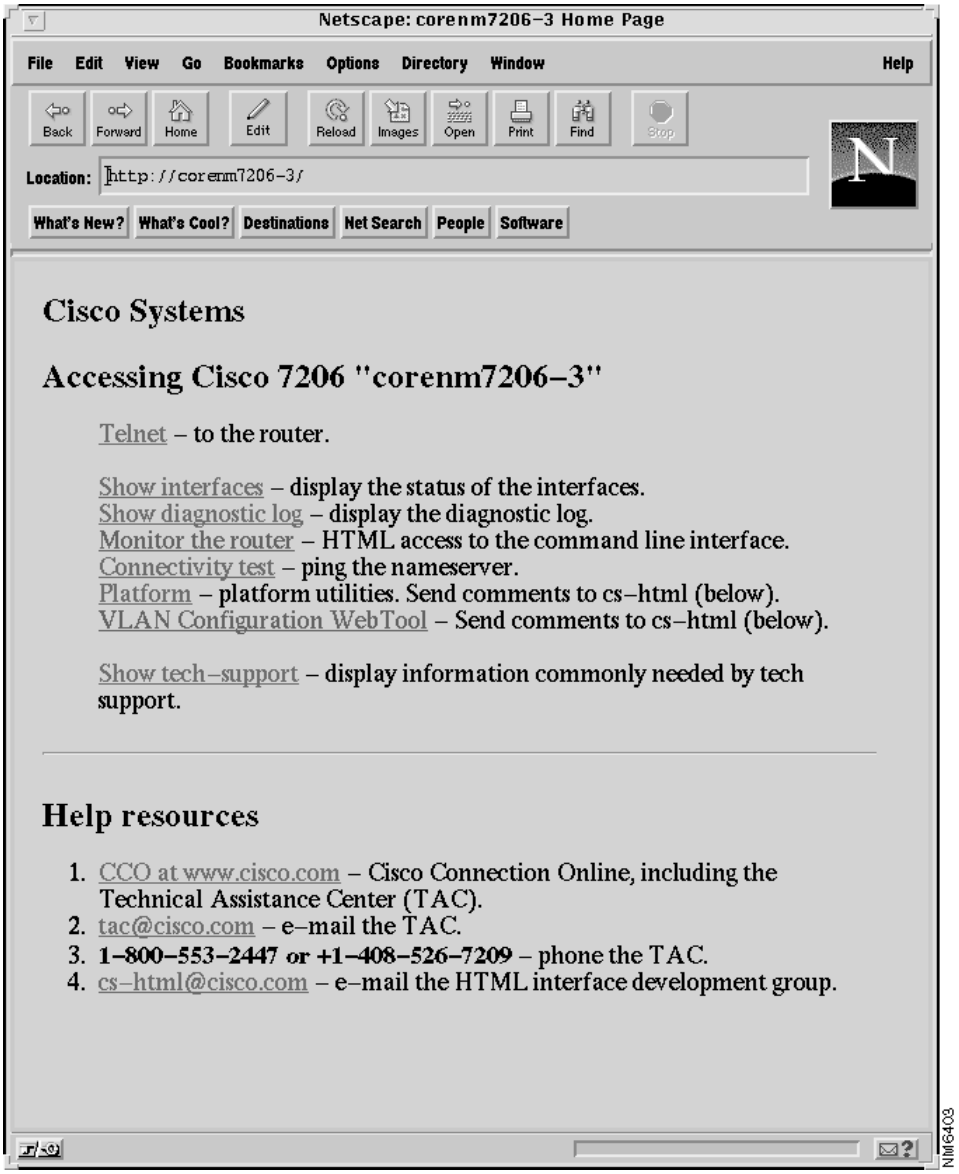
Configuring Bridge Groups Using the 12E/2FE VLAN Configuration WebTool

The 12E/2FE VLAN Configuration WebTool, shown in Figure 2, is a web browser-based Java applet that displays configured interfaces and bridge groups for PA-12E/2FE port adapters installed in Cisco routers. With the WebTool you can perform the following tasks:

- Create and delete bridge groups (also referred to as VLANs)
- Add and remove PA-12E/2FE interfaces from bridge groups
- Assign colors to bridge groups and PA-12E/2FE interfaces
- Administratively shut down (disable) and bring up (enable) PA-12E/2FE interfaces
- View the bridge-group status of each PA-12E/2FE interface

You can access the 12E/2FE VLAN Configuration WebTool from the home page of your router. For complete procedures on how to use the VLAN Configuration WebTool, refer to the *PA-12E/2FE Ethernet Switch Port Adapter* book that accompanies the hardware.

Figure 2 Example Home Page for a Cisco 7200 Series Router (Cisco 7206 Shown)



Location: http://corenm7206-3/

Cisco Systems

Accessing Cisco 7206 "corenm7206-3"

Telnet – to the router.

Show interfaces – display the status of the interfaces.
Show diagnostic log – display the diagnostic log.
Monitor the router – HTML access to the command line interface.
Connectivity test – ping the nameserver.
Platform – platform utilities. Send comments to cs–html (below).
VLAN Configuration WebTool – Send comments to cs–html (below).

Show tech–support – display information commonly needed by tech support.

Help resources

1. CCO at www.cisco.com – Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com – e–mail the TAC.
3. **1–800–553–2447 or +1–408–526–7209** – phone the TAC.
4. cs–html@cisco.com – e–mail the HTML interface development group.

All Cisco routers that run Cisco IOS Release 11.0 or later have a home page. All Cisco router home pages are password protected. Contact your network administrator if you do not have the name or password for your Cisco 7200 series router.

If your router has an installed PA-12E/2FE port adapter, the 12E/2FE VLAN Configuration WebTool shown in Figure 2 can be accessed from the home page of the router using a Java-enabled web browser.

Configuring the 100VG-AnyLAN Port Adapter

The 100VG-AnyLAN port adapter (PA-100VG) is available on Cisco 7200 series routers and on Cisco 7500 series routers.

The PA-100VG provides a single interface compatible with and specified by IEEE 802.12 to support 100 Mbps over Category 3 or Category 5 UTP cable with RJ-45 terminators. The PA-100VG supports 802.3 Ethernet packets and can be monitored with the IEEE 802.12 Interface MIB.

To configure the PA-100VG port adapter, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	`Router(config)#` **`interface vg-anylan`** *`slot/port`* (Cisco 7200) or `Router(config)#` **`interface vg-anylan`** *`slot/port-adapter/port`* (Cisco 7500)	Specifies a 100VG-AnyLAN interface and enters interface configuration.
Step 2	`Router(config-if)#` **`ip address`** *`ip-address mask`*	Specifies the IP address and subnet mask to the interface.
Step 3	`Router(config-if)#` **`frame-type ethernet`**	Configures the frame type. Currently, only Ethernet frames are supported. The frame type defaults to Ethernet.

Note The port number for the 100VG-AnyLAN port adapter is always 0.

Configuring the PA-100VG interface is similar to configuring an Ethernet or Fast Ethernet interface. To display information about the 100VG-AnyLAN port adapter, use the **show interfaces vg-anylan** EXEC command.

Configuring the Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers

The Cisco 7200-I/O-GE+E is an Input/Output controller that provides one Gigabit Ethernet and one Ethernet port. It is equipped with a GBIC receptacle for 1000-Mbps operation and an RJ-45 receptacle for 10-Mbps operation.

The Cisco 7200-I/O-2FE/E is an Input/Output controller that provides two autosensing Fast Ethernet ports and is equipped with two RJ-45 receptacles for 10/100-Mbps operation.

I/O controllers support the following features:

- Dual EIA/TIA-232 channels for local console and auxiliary ports
- NVRAM for storing the system configuration and environmental monitoring logs
- Two PC Card slots that hold Flash disks or Flash memory cards for storing the default Cisco IOS software image

- Flash memory for storing the boot helper image
- Two environmental sensors for monitoring the cooling air as it enters and leaves the chassis

Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Configuration Task List

See the following sections for configuration tasks for the Cisco 7200-I/O-GE+E and the Cisco 7200-I/O-2FE/E feature. Each task in the list is identified as required or optional.

- Configuring the Interface Transmission Mode, page 45 (Optional)
- Configuring Interface Speed, page 46 (Optional)
- Configuring the Ethernet, Fast Ethernet, and Gigabit Ethernet Interfaces, page 46 (Required)
- Verifying the Configuration, page 47 (Optional)
- Monitoring and Maintaining the Cisco 7200-I/O GE+E and Cisco 7200-I/O-2FE/E, page 48 (Optional)

Note For Cisco 7200 VXR routers used as router shelves in AS5800 Universal Access Servers, use the *router-shelf***/***slot***/***port* command format for all interface commands.

Configuring the Interface Transmission Mode

To configure the interface transmission mode, use the following commands beginning in privileged EXEC mode. The Fast Ethernet and Ethernet interfaces on the Cisco 7200-I/O-2FE/E are duplex auto by default.

	Command or Action	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode and specifies that the console terminal is the source of the configuration subcommands.
Step 2	`Router(config)# interface fastethernet 0/0`[1]	Selects the Fast Ethernet interface to configure.
Step 3	`Router(config)# duplex full`	Changes the Fast Ethernet interface port transmission mode to full duplex from autonegotiation.

[1] Use the **interface fastethernet** *router-shelf***/***slot***/***port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

Configuring Interface Speed

To configure the two autosensing Ethernet/Fast Ethernet interfaces on the C7200-I/O-2FE/E, use the **speed** command. The the default interface speed is auto. The following procedure configures the C7200-I/O-2FE/E for a speed of 10 Mbps.

	Command or Action	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode and specifies that the console terminal is the source of the configuration subcommands.
Step 2	`Router(Config)# interface ethernet 0/1`[1]	Selects the Ethernet interface to configure.
	`Router(Config-if)# interface fastethernet 0/0`[2]	Selects the Fast Ethernet interface to configure.
Step 3	`Router(Config-if)# speed 10`	Sets the Ethernet or Fast Ethernet interface speed to 10 Mbps.

[1] Use the **interface ethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

[2] Use the **interface fastethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

Configuring the Ethernet, Fast Ethernet, and Gigabit Ethernet Interfaces

The following procedure explains a basic configuration for an Ethernet, Fast Ethernet, or Gigabit Ethernet interface on a C7200-I/O-GE+E or a C7200-I/O-2FE/E.

	Command or Action	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode and specifies that the console terminal is the source of the configuration subcommands.
Step 2	`Router(config)# interface ethernet 0/1`[1]	Selects the Ethernet interface on the I/O controller in slot 0 in port adapter slot 1 to configure.
	`Router(config)# interface fastethernet 0/1`[2]	Selects the Fast Ethernet interface on the I/O controller in slot 0 in port adapter slot 2 to configure.
	`Router(config)# interface gigabitethernet 0/0`[3]	Selects the Gigabit Ethernet interface on the I/O controller in slot 0 in port adapter slot 0 to configure.
Step 3	`Router(config-if) # ip address 10.1.1.10 255.255.255.0`	Assigns an IP address and subnet mask to the interface (if IP routing is enabled on the system).
Step 4	`Router(config-if)# duplex auto`	Changes the Fast Ethernet interface port transmission mode to autonegotiation.
Step 5	`Router#(config-if)# Ctrl-Z`	Exits configuration mode.

[1] Use the **interface ethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

[2] Use the **interface fastethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

[3] Use the **interface gigabitethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

Verifying the Configuration

Use the **show interfaces** {**ethernet** | **fastethernet** | **gigabitethernet**} command to verify that the interface and line protocol are in the correct state (up) and that the transmission mode is configured on the interface. You can configure full, half, or auto transmission mode for Ethernet and Fast Ethernet interfaces. You can configure forced transmission mode for Gigabit Ethernet interfaces. The following is sample output from the **show interfaces gigabitethernet** command.

```
Router# show interfaces gigabitethernet 0/0

GigabitEthernet0/0 is up, line protocol is up
   Hardware is 82543 (Livengood), address is 00d0.ffb6.4c00 (bia 00d0.ffb6.4c00)
   Internet address is 10.1.1.0/0
   MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   Full-duplex mode, link type is autonegotiation, media type is SX
   output flow-control is on, input flow-control is on
   ARP type:ARPA, ARP Timeout 04:00:00
   Last input 00:00:04, output 00:00:03, 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
      2252 packets input, 135120 bytes, 0 no buffer
      Received 2252 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 0 multicast, 0 pause input
      0 input packets with dribble condition detected
      2631 packets output, 268395 bytes, 0 underruns
      0 output errors, 0 collisions, 2 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier, 0 pause output
      0 output buffer failures, 0 output buffers swapped out
```

Monitoring and Maintaining the Cisco 7200-I/O GE+E and Cisco 7200-I/O-2FE/E

To monitor and maintain the Gigabit Ethernet or Ethernet interfaces on the Cisco 7200-I/O-GE+E, use the following commands in privileged EXEC mode.

Command or Action	Purpose
`Router# show controllers ethernet`	Displays hardware and software information about the Ethernet interface.
`Router# show interfaces ethernet slot/port`[1]	Displays information about the Ethernet interface on the router.
`Router# show controllers gigabitethernet`	Displays hardware and software information about the Gigabit Ethernet interface.
`Router# show interfaces gigabitethernet slot/port`[2]	Displays information about a Gigabit Ethernet interface on the router.

1. Use the **show interfaces ethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server
2. Use the **interface gigabitethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

To monitor and maintain the Fast Ethernet or Ethernet interfaces on the Cisco 7200-I/O-2FE/E, use the following commands in privileged EXEC mode.

Command or Action	Purpose
`Router# show controllers ethernet`	Displays hardware and software information about the Ethernet interface.
`Router# show interfaces ethernet slot/port`[1]	Displays information about an Ethernet interface on the router.
`Router# show controllers fastethernet`	Displays hardware and software information about the Fast Ethernet interfaces.
`Router# show interfaces fastethernet`	Displays information about a Fast Ethernet interface on the router.

1. Use the **show interfaces ethernet** *router-shelf/slot/port* command for a Cisco 7200 VXR used as a router shelf in an AS5800 Universal Access Server.

Configuring Fast EtherChannel

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. Fast EtherChannel builds on standards-based 802.3 full-duplex Fast Ethernet to provide fault-tolerant, high-speed links between switches, routers, and servers. This feature can be configured between Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) or between a Cisco 7500 series router or a Cisco 7000 series router with the RSP7000 and RSP7000CI and a Catalyst 5000 switch.

Note Using the Fast EtherChannel feature on a Catalyst 5000 switch requires a hardware upgrade. Contact your local sales representative for upgrade details.

Fast EtherChannel provides higher bidirectional bandwidth, redundancy, and load sharing. Up to four Fast Ethernet interfaces can be bundled in a port channel, and the router or switch can support up to four port channels. The Fast EtherChannel feature is capable of load balancing traffic across the Fast Ethernet links. Unicast, broadcast, and multicast traffic is distributed across the links providing higher performance and redundant parallel paths. In the event of a link failure, traffic is redirected to remaining links within the Fast EtherChannel without user intervention.

Fast EtherChannel feature, IP traffic is distributed over the port channel interface while traffic from other routing protocols is sent over a single link. Bridged traffic is distributed on the basis of the Layer 3 information in the packet. If the Layer 3 information does not exist in the packet, the traffic is sent over the first link.

Fast EtherChannel supports all features currently supported on the Fast Ethernet interface. You must configure these features on the port-channel interface rather than on the individual Fast Ethernet interfaces. Fast EtherChannel connections are fully compatible with Cisco IOS VLAN and routing technologies. The Inter-Switch Link (ISL) VLAN trunking protocol can carry multiple VLANs across a Fast EtherChannel, and routers attached to Fast EtherChannel links can provide full multiprotocol routing with support for host standby using Hot Standby Router Protocol (HSRP).

The port channel (consisting of up to four Fast Ethernet interfaces) is treated as a single interface. A port channel is used in the Cisco IOS software to maintain compatibility with existing commands on the Catalyst 5000 switch. You create the Fast EtherChannel by using the **interface port-channel** interface configuration command. You can assign up to four Fast Ethernet interfaces to a port channel by using the **channel-group** interface configuration command.

Additional Fast EtherChannel features include

- Hot Standby Router Protocol (HSRP)

  For more information about configuring HSRP, refer to the "Configuring IP Services" chapter in the *Cisco IOS IP Application Services Configuration Guide*.

- Cisco Express Forwarding (CEF) and distributed CEF (dCEF)

  For more information about configuring CEF, refer to the "Configuring Cisco Express Forwarding" part of the *Cisco IOS IP Switching Configuration Guide.*

For information on how to configure Ethernet or Fast Ethernet, see the tasks listed in the "Configuring the Ethernet, Fast Ethernet, and Gigabit Ethernet Interfaces" section on page 46.

Fast EtherChannel Configuration Task List

To configure Fast EtherChannel, perform the tasks in the following sections. Each task is identified as required or optional.

- Configuring the Port-Channel Interface, page 50
- Configuring the Fast Ethernet Interfaces, page 51

For information on other commands that can be used by the Fast EtherChannel, refer to the other configuration guides and command references in the Cisco IOS documentation set.

Configuring the Port-Channel Interface

To configure the port-channel interface, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	Router(config)# **interface port-channel** *channel-number*	Creates the port-channel interface and enters interface configuration mode. The channel number can be 1 to 4.
Step 2	Router(config-if)# **ip address** *ip-address mask*	Assigns an IP address and subnet mask to the Fast EtherChannel. If you configure ISL, you must assign the IP address to the subinterface (for example, interface port channel 1.1—an IP address per VLAN) and you must specify the encapsulation with VLAN number under that subinterface (for example, encapsulation isl 100).
Step 3	Router(config-if)# **mac-address** *ieee-address*	(Optional) Assigns a static MAC address to the Fast EtherChannel. If you do not assign a static MAC address on the port-channel interface, the Cisco IOS software automatically assigns a MAC address. If you assign a static MAC address and then later remove it, the Cisco IOS software automatically assigns a MAC address.
Step 4	Router(config-if)# **end**	(Optional) Enables other supported interface commands to execute, and exits when they have finished.
Step 5	Router# **show interface port-channel**	Displays information about the port-channel interface so that you can verify the configuration.

Note If you want to use the Cisco Discovery Protocol (CDP), you must configure it on the physical Ethernet, Fast Ethernet, or Gigabit Ethernet interface, not on the port-channel interface.

Caution With Release 11.1(20)CC and later, Fast EtherChannel supports CEF/dCEF. We recommend that you clear all explicit **ip route-cache distributed** commands from the Fast Ethernet interfaces before enabling dCEF on the port-channel interface. Doing this gives the port-channel interface proper control of its physical Fast Ethernet links. When you enable CEF/dCEF globally, all interfaces that support CEF/dCEF are enabled. When CEF/dCEF is enabled on the port-channel interface, it is automatically enabled on each of the Fast Ethernet interfaces in the channel group. However, if you have previously disabled CEF/dCEF on the Fast Ethernet interface, CEF/dCEF is not automatically enabled. In this case, you must enable CEF/dCEF on the Fast Ethernet interface.

Configuring the Fast Ethernet Interfaces

To assign the Fast Ethernet interfaces to the Fast EtherChannel, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	Router(config)# **interface fastethernet** *slot/port* (Cisco 7200 series routers) Router(config)# **interface fastethernet** *slot/port-adapter/port* (Cisco 7500 series and Cisco 7000 series routers with RSP7000)	Creates or modifies an existing Fast Ethernet interface and enters interface configuration mode.
Step 2	Router(config-if)# **no ip address**	Disables the IP address before performing the next step, if the Fast Ethernet interface already exists and has an IP address assigned.
Step 3	Router(config-if)# **channel-group** *channel-number*	Assigns the Fast Ethernet interfaces to the Fast EtherChannel. The channel number is the same as the channel number that you specified when you created the port-channel interface.
Step 4	Router(config-if)# **exit**	Exits interface configuration mode. Repeat Steps 1 through 4 to add up to four Fast Ethernet interfaces to the Fast EtherChannel.
Step 5	Router(config-if)# **end**	(Optional) Enables other supported interface commands to execute, and exits when they have finished.
Step 6	Router(config)# **show interfaces port-channel**	Displays information about the Fast Ethernet interface so that you can verify the configuration.

Caution The port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces. Do not assign bridge groups on the physical Fast Ethernet interfaces because it creates loops. Also, you must disable spanning tree.

To remove a Fast Ethernet interface from a Fast EtherChannel, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	Router(config)# **interface fastethernet** *slot/port* (Cisco 7200 series routers) Router(config)# **interface fastethernet** *slot/port-adapter/port* (Cisco 7500 series and Cisco 7000 series routers with RSP7000)	Specifies the Fast Ethernet interface and enters interface configuration mode.
Step 2	Router(config-if)# **no channel-group**	Removes the Fast Ethernet interface from the channel group.
Step 3	Router(config-if)# **end**	(Optional) Enables other supported interface commands to execute, and exits when they have finished.

The Cisco IOS software automatically removes a Fast Ethernet interface from the Fast EtherChannel if the interface goes down, and the software automatically adds the Fast Ethernet interface to the Fast EtherChannel when the interface is back up.

Currently, Fast EtherChannel relies on keepalives to detect whether the line protocol is up or down. Keepalives are enabled by default on the Fast Ethernet interfaces. If the line protocol on the interface goes down because it did not receive a keepalive signal, the Fast EtherChannel detects that the line protocol is down and removes the interface from the Fast EtherChannel. However, if the line protocol remains up because keepalives are disabled on the Fast Ethernet interface, the Fast EtherChannel cannot detect this link failure (other than a cable disconnect) and does not remove the interface from the Fast EtherChannel even if the line protocol goes down. This can result in unpredictable behavior. The implementation of the Port Aggregation Protocol in a subsequent release of this feature will remove the dependency on keepalives.

See the "LAN Interface Configuration Examples" section on page 66 for configuration examples.

You can monitor the status of the Fast EtherChannel interface by using the **show interfaces port-channel** EXEC command.

Configuring the Gigabit Ethernet Interfaces

To assign the Gigabit Ethernet interfaces to the Gigabit EtherChannel, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	`Router(config)#` **`interface gigabitethernet`** *`slot/port`* (Cisco 7200 series routers)	Creates or modifies an existing Gigabit Ethernet interface and enters interface configuration mode.
Step 2	`Router(config-if)#` **`no ip address`**	Disables the IP address before performing the next step, if the Gigabit Ethernet interface already exists and has an IP address assigned.
Step 3	`Router(config-if)#` **`channel-group`** *`channel-number`*	Assigns the Gigabit Ethernet interfaces to the Gigabit EtherChannel. The channel number is the same as the channel number that you specified when you created the port-channel interface.
Step 4	`Router(config-if)#` **`exit`**	Exits interface configuration mode. Repeat Steps 1 through 4 to add up to eight Gigabit Ethernet interfaces to the Gigabit EtherChannel.
Step 5	`Router(config-if)#` **`end`**	(Optional) Enables other supported interface commands to execute, and exits when they have finished.
Step 6	`Router(config)#` **`show interfaces port-channel`**	Displays information about the Gigabit Ethernet interface so that you can verify the configuration.

To remove a Gigabit Ethernet interface from a Gigabit EtherChannel, use the following commands beginning in global configuration mode.

	Command or Action	Purpose
Step 1	`Router(config)#` **`interface gigabitethernet`** *`slot/port`* (Cisco 7200 series routers)	Specifies the Gigabit Ethernet interface and enters interface configuration mode.

	Command or Action	Purpose
Step 2	`Router(config-if)#` **`no channel-group`**	Removes the Gigabit Ethernet interface from the channel group.
Step 3	`Router(config-if)#` **`end`**	(Optional) Enables other supported interface commands to execute, and exits when they have finished.

You can monitor the status of the Gigabit EtherChannel interface by using the **show interfaces port-channel** EXEC command.

Configuring a FDDI Interface

The FDDI is an ANSI-defined standard for timed 100-Mbps token passing over fiber-optic cable. FDDI is not supported on access servers.

A FDDI network consists of two counter-rotating, token-passing fiber-optic rings. On most networks, the primary ring is used for data communication and the secondary ring is used as a hot standby. The FDDI standard sets a total fiber length of 200 kilometers. (The maximum circumference of the FDDI network is only half the specified kilometers because of the *wrapping* or looping back of the signal that occurs during fault isolation.)

The FDDI standard allows a maximum of 500 stations with a maximum distance between active stations of 2 kilometers when interconnecting them with multimode fiber or 10 kilometers when interconnected via single mode fiber, both of which are supported by our FDDI interface controllers. The FDDI frame can contain a minimum of 17 bytes and a maximum of 4500 bytes. Our implementation of FDDI supports Station Management (SMT) Version 7.3 of the X3T9.5 FDDI specification, offering a single MAC dual-attach interface that supports the fault-recovery methods of the dual attachment stations (DASs). The mid-range platforms also support single attachment stations (SASs).

Refer to the *Cisco Product Catalog* for specific information on platform and interface compatibility. For installation and configuration information, refer to the installation and configuration publication for the appropriate interface card or port adapter.

Source-Route Bridging over FDDI on Cisco 4000-M, Cisco 4500-M, and Cisco 4700-M Routers

Source-route bridging (SRB) is supported on the FDDI interface to the Cisco 4000-M, Cisco 4500-M, and Cisco 4700-M routers. For instructions on configuring autonomous FDDI SRB or fast-switching SRB over FDDI, refer to the "Configuring Source-Route Bridging" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

Particle-Based Switching of Source-Route Bridge Packets on Cisco 7200 Series Routers

SRB is supported over FDDI. Particle-based switching is supported for SRB packets (over FDDI and Token Ring) by default.

Particle-based switching adds scatter-gather capability to SRB to improve performance. Particles represent a communications data packet as a collection of noncontiguous buffers. The traditional Cisco IOS packet has a packet type control structure and a single contiguous data buffer. A particle packet has the same packet type control structure, but also maintains a queue of particle type structures, each of which manages its own block.

The scatter-gather architecture used by particle-based switching provides the following advantages:

- Allows drivers to use memory more efficiently (especially when using media that has a large maximum transmission unit [MTU]). For example, Token Ring buffers could be 512 bytes rather than 16 KB.
- Allows concurrent use of the same region of memory. For example, on IP multicast a single packet is received and sent out on multiple interfaces simultaneously.
- Allows insertion or deletion of memory at any location in a packet (not just at the beginning or end).

For information about configuring SRB over FDDI, refer to the "Configuring Source-Route Bridging" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

Using Connection Management Information

Connection management (CMT) is a FDDI process that handles the transition of the ring through its various states (off, on, active, connect, and so on) as defined by the X3T9.5 specification. The FIP (FDDI Interface Processor) provides CMT functions in microcode.

A partial sample output of the **show interfaces fddi** command follows, along with an explanation of how to interpret the CMT information in the output.

```
Phy-A state is active, neighbor is B, cmt signal bits 08/20C, status ALS
Phy-B state is active, neighbor is A, cmt signal bits 20C/08, status ILS
CFM is thru A, token rotation 5000 usec, ring operational 0:01:42
Upstream neighbor 0800.2008.C52E, downstream neighbor 0800.2008.C52E
```

The **show interfaces fddi** example shows that Physical A (Phy-A) completed CMT with its neighbor. The state is active, and the display indicates a Physical B-type neighbor.

The sample output indicates CMT signal bits 08/20C for Phy-A. The transmit signal bits are 08. Looking at the pulse code modulation (PCM) state machine, 08 indicates that the port type is A, that the port compatibility is set, and that the LCT duration requested is short. The receive signal bits are 20C, that indicate that the neighbor type is B, that port compatibility is set, that there is a MAC on the port output, and so on.

The neighbor is determined from the received signal bits, as follows:

Bit Positions	9	8	7	6	5	4	3	2	1	0
Value Received	1	0	0	0	0	0	1	1	0	0

Interpreting the bits in the diagram above, the received value equals 0x20C. Bit positions 1 and 2 (0 1) indicate a Physical B-type connection.

The transition states displayed indicate that the CMT process is running and actively trying to establish a connection to the remote physical connection. The CMT process requires state transition with different signals being transmitted and received before moving on to the state ahead as indicated in the PCM state machine. The 10 bits of CMT information are transmitted and received in the Signal State. The NEXT state is used to separate the signaling performed in the Signal State. Therefore, in the preceding sample output, the NEXT state was entered 11 times.

Note The display line showing transition states is not generated if the FDDI interface has been shut down, or if the **cmt disconnect** command has been issued, or if the **fddi if-cmt** command has been issued. (The **fddi if-cmt** command applies to the Cisco 7500 series routers only.)

The CFM state is through A in the sample output, which means the Phy-A of this interface has successfully completed CMT with the Phy-B of the neighbor and Phy-B of this interface has successfully completed CMT with the Phy-A of the neighbor.

The display (or nondisplay) of the upstream and downstream neighbor does not affect the ability to route data. Because the upstream neighbor is also its downstream neighbor in the sample, there are only two stations in the ring: the network server and the router at address 0800.2008.C52E.

FDDI Configuration Task List

To configure a FDDI interface, perform the tasks in the following sections. Each task in the list is identified as either required or optional.

- Specifying a FDDI Interface, page 55 (Required)
- Enabling FDDI Bridging Encapsulation, page 56 (Optional)
- Enabling Full-Duplex Mode on the FDDI Interface, page 57 (Optional)
- Setting the Token Rotation Time, page 57 (Optional)
- Setting the Transmission Valid Timer, page 57 (Optional)
- Controlling the Transmission Timer, page 57 (Optional)
- Modifying the C-Min Timer, page 58 (Optional)
- Modifying the TB-Min Timer, page 58 (Optional)
- Modifying the FDDI Timeout Timer, page 58 (Optional)
- Controlling SMT Frame Processing, page 58 (Optional)
- Enabling Duplicate Address Checking, page 58 (Optional)
- Setting the Bit Control, page 59 (Optional)
- Controlling the CMT Microcode, page 59 (Optional)
- Starting and Stopping FDDI, page 59 (Optional)
- Setting FDDI Frames per Token Limit, page 59 (Optional)
- Controlling the FDDI SMT Message Queue Size, page 60 (Optional)
- Preallocating Buffers for Bursty FDDI Traffic, page 60 (Optional)

Specifying a FDDI Interface

To specify a FDDI interface and enter interface configuration mode, use one of the following commands in global configuration mode.

Command or Action	Purpose
`Router(config)# interface fddi number`	Enters interface configuration.
`Router(config)# interface fddi slot/port`	Enters interface configuration for the Cisco 7200 or Cisco 7500 series routers.

Enabling FDDI Bridging Encapsulation

By default, Cisco FDDI uses the SNAP encapsulation format defined in RFC 1042. It is not necessary to define an encapsulation method for this interface when using the FIP.

FIP fully supports transparent and translational bridging for the following configurations:

- FDDI-to-FDDI
- FDDI-to-Ethernet
- FDDI-to-Token Ring

Enabling FDDI bridging encapsulation places the FIP into encapsulation mode when doing bridging. In transparent mode, the FIP interoperates with earlier versions of encapsulating interfaces when performing bridging functions on the same ring. When using the FIP, you can specify the encapsulation method by using the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi encapsulate`	Specifies the encapsulation method for the FIP.

When you are doing translational bridging, use routing for routable protocols and use translational bridging for the rest, such as local-area transport (LAT).

Note Bridging between dissimilar media presents several problems that can prevent communications. These problems include bit-order translation (using MAC addresses as data), maximum transfer unit (MTU) differences, frame status differences, and multicast address usage. Some or all of these problems might be present in a multimedia-bridged LAN and might prevent communication. These problems are most prevalent in networks that bridge between Token Ring and Ethernet networks or between Token Ring and FDDI because of the different ways that Token Ring is implemented by the end nodes.

We are currently aware of problems with the following protocols when bridged between Token Ring and other media: AppleTalk, DECnet, IP, Novell IPX, Phase IV, VINES, and XNS. Further, the following protocols might have problems when bridged between FDDI and other media: Novell IPX and XNS. We recommend that these protocols be routed whenever possible.

Enabling Full-Duplex Mode on the FDDI Interface

To enable full-duplex mode on the PA-F/FD-SM and PA-F/FD-MM port adapters, use one of the following commands in interface configuration mode.

Command or Action	Purpose

`Router(config-if)# full-duplex`
or
`Router(config-if)# no half-duplex`
	Enables full-duplex on the FDDI interface of the PA-F/FD-SM and PA-F/FD-MM port adapter.

Setting the Token Rotation Time

You can set the FDDI token rotation time to control ring scheduling during normal operation and to detect and recover from serious ring error situations. To do so, use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi token-rotation-time microseconds`	Sets the FDDI token rotation time.

The FDDI standard restricts the allowed time to greater than 4000 microseconds and less than 165,000 microseconds. As defined in the X3T9.5 specification, the value remaining in the token rotation timer (TRT) is loaded into the token holding timer (THT). Combining the values of these two timers provides the means to determine the amount of bandwidth available for subsequent transmissions.

Setting the Transmission Valid Timer

You can set the transmission timer to recover from a transient ring error by using the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi valid-transmission-time microseconds`	Sets the FDDI valid transmission timer.

Controlling the Transmission Timer

You can set the FDDI control transmission timer to control the FDDI TL-Min time, which is the minimum time to transmit a Physical Sublayer or PHY line state before advancing to the next Physical Connection Management or PCM state as defined by the X3T9.5 specification. To do so, use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi tl-min-time microseconds`	Sets the FDDI control transmission timer.

Modifying the C-Min Timer

You can modify the C-Min timer on the PCM from its default value of 1600 microseconds by using the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi c-min microseconds`	Sets the C-Min timer on the PCM.

Modifying the TB-Min Timer

You can change the TB-Min timer in the PCM from its default value of 100 milliseconds. To do so, use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi tb-min milliseconds`	Sets TB-Min timer in the PCM.

Modifying the FDDI Timeout Timer

You can change the FDDI timeout timer in the PCM from its default value of 100 ms. To do so, use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi t-out milliseconds`	Sets the timeout timer in the PCM.

Controlling SMT Frame Processing

You can disable and enable SMT frame processing for diagnostic purposes. To do so, use one of the following commands in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# no fddi smt-frames`	Disables SMT frame processing.
`Router(config-if)# fddi smt-frames`	Enables SMT frame processing.

Enabling Duplicate Address Checking

You can enable the duplicate address detection capability on the FDDI. If the FDDI finds a duplicate address, it displays an error message and shuts down the interface. To enable duplicate address checking, use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi duplicate-address-check`	Enables duplicate address checking capability.

Setting the Bit Control

You can set the FDDI bit control to control the information transmitted during the Connection Management (CMT) signaling phase. To do so, use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi cmt-signal-bits signal-bits [phy-a | phy-b]`	Sets the FDDI bit control.

Controlling the CMT Microcode

You can control whether the CMT onboard functions are on or off. The FIP provides CMT functions in microcode. These functions are separate from those provided on the processor card and are accessed through EXEC commands.

The default is for the FIP CMT functions to be on. A typical reason to disable these functions is when you work with new FDDI equipment and have problems bringing up the ring. If you disable the CMT microcode, the following actions occur:

- The FIP CMT microcode is disabled.
- The main system code performs the CMT function while debugging output is generated.

To disable the CMT microcode, use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# no fddi if-cmt`	Disables the FCIT CMT functions.

Starting and Stopping FDDI

In normal operation, the FDDI interface is operational once the interface is connected and configured. You can start and stop the processes that perform the CMT function and allow the ring on one fiber to be stopped. To do so, use either of the following commands in EXEC mode.

Command or Action	Purpose
`Router# cmt connect [interface-name [phy-a | phy-b]]`	Starts CMT processes on a FDDI ring.
`Router# cmt disconnect [interface-name [phy-a | phy-b]]`	Stops CMT processes on a FDDI ring.

Do not use either of the preceding commands during normal operation of FDDI; they are used during interoperability tests.

Setting FDDI Frames per Token Limit

The FDDI interface is able to transmit multiple frames per token on a Cisco 4000, a Cisco 4500, and a Cisco 4700 series router, instead of transmitting only a single frame at a time. You can specify the maximum number of frames to be transmitted with each token capture. This significantly improves your throughput when you have heavy or very bursty traffic.

To configure the FDDI interface to transmit a maximum number of frames per token capture, use the following commands beginning in privileged EXEC mode.

	Command or Action	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# interface fddi0`	Enters interface configuration mode.
Step 3	`Router(config-if)# fddi ?`	Shows **fddi** command options.
Step 4	`Router(config-if)# fddi frames-per-token ?`	Shows **fddi frames-per-token** command options.
Step 5	`Router(config-if)# fddi frames-per-token number`	Specifies the maximum number of frames to be transmitted per token capture.

Controlling the FDDI SMT Message Queue Size

You can set the maximum number of unprocessed FDDI Station Management (SMT) frames that will be held for processing. Setting this number is useful if the router that you are configuring gets bursts of messages that arrive faster than the router can process. To set the number of frames, use the following command in global configuration mode.

Command or Action	Purpose
`Router(config)# smt-queue-threshold number`	Sets SMT message queue size.

Preallocating Buffers for Bursty FDDI Traffic

The FCI card preallocates three buffers to handle bursty FDDI traffic (for example, Network File System (NFS) bursty traffic). You can change the number of preallocated buffers use the following command in interface configuration mode.

Command or Action	Purpose
`Router(config-if)# fddi burst-count`	Preallocates buffers to handle bursty FDDI traffic.

Configuring a Hub Interface

Cisco 2500 series includes routers that have hub functionality for an Ethernet interface. The hub is a multiport repeater. The advantage of an Ethernet interface over a hub is that the hub provides a star-wiring physical network configuration while the Ethernet interface provides 10BASE-T physical network configuration. The router models with hub ports and their configurations are as follows:

- Cisco 2505—1 Ethernet (8 ports) and 2 serial
- Cisco 2507—1 Ethernet (16 ports) and 2 serial
- Cisco 2516—1 Ethernet (14 ports), 2 serial, and 1 ISDN BRI

Cisco provides Simple Network Management Protocol (SNMP) management of the Ethernet hub as specified in RFC 1516, *Definitions of Managed Objects for IEEE 802.3 Repeater Devices*.

To configure hub functionality on an Ethernet interface, perform the tasks in the following sections Each task in the list is identified as either required or optional.

- Enabling a Hub Port, page 61 (Required)
- Disabling or Enabling Automatic Receiver Polarity Reversal, page 61 (Optional)
- Disabling or Enabling the Link Test Function, page 61 (Optional)
- Enabling Source Address Control, page 62 (Optional)
- Enabling SNMP Illegal Address Trap, page 63 (Optional)

For configuration examples, see the "Hub Configuration Examples" section on page 71.

Enabling a Hub Port

To enable a hub port, use the following commands in global configuration mode.

	Command or Action	Purpose
Step 1	`Router(config)# hub ethernet number port [end-port]`	Specifies the hub number and the hub port (or range of hub ports) and enters hub configuration mode.
Step 2	`Router(config)# no shutdown`	Enables the hub ports.

Disabling or Enabling Automatic Receiver Polarity Reversal

On Ethernet hub ports only, the hub ports can invert, or correct, the polarity of the received data if the port detects that the received data packet waveform polarity is reversed because of a wiring error. This receive circuitry polarity correction allows the hub to repeat subsequent packets with correct polarity. When enabled, this function is executed once after reset of a link fail state.

Automatic receiver polarity reversal is enabled by default. To disable this feature on a per-port basis, use the following command in hub configuration mode.

Command or Action	Purpose
`Router(config-hub)# no auto-polarity`	Disables automatic receiver polarity reversal.

To enable automatic receiver polarity reversal on a per-port basis, use the following command in hub configuration mode.

Command or Action	Purpose
`Router(config-hub)# auto-polarity`	Enables automatic receiver polarity reversal.

Disabling or Enabling the Link Test Function

The link test function applies to Ethernet hub ports only. The Ethernet ports implement the link test function as specified in the 802.3 10BASE-T standard. The hub ports will transmit link test pulses to any attached twisted pair device if the port has been inactive for more than 8 to 17 milliseconds.

If a hub port does not receive any data packets or link test pulses for more than 65 to 132 milliseconds and the link test function is enabled for that port, that port enters link fail state and cannot transmit or receive. The hub port is enabled again when it receives four consecutive link test pulses or a data packet.

The link test function is enabled by default. To allow the hub to interoperate with 10BASE-T twisted-pair networks that do not implement the link test function, the link test receive function of the hub can be disabled on a per-port basis. To do so, use the following command in hub configuration mode.

Command	Purpose
`Router(config-hub)# no link-test`	Disables the link test function.

To enable the link test function on a hub port connected to an Ethernet interface, use the following command in hub configuration mode.

Command	Purpose
`Router(config-hub)# link-test`	Enables the link test function.

Enabling Source Address Control

On an Ethernet hub port only, you can configure a security measure such that the port accepts packets only from a specific MAC address. For example, suppose your workstation is connected to port 3 on a hub, and source address control is enabled on port 3. Your workstation has access to the network because the hub accepts any packet from port 3 with the MAC address of the workstation. Any packets that arrive with a different MAC address cause the port to be disabled. The port is enabled again after 1 minute, and the MAC address of incoming packets is checked again.

To enable source address control on a per-port basis, use the following command in hub configuration mode.

Command	Purpose
`Router(config-hub)# source-address [mac-address]`	Enables source address control.

If you omit the optional MAC address, the hub remembers the first MAC address that it receives on the selected port and allows only packets from the learned MAC address.

See the examples of establishing source address control in the "Hub Configuration Examples" section on page 71.

Enabling SNMP Illegal Address Trap

To enable the router to issue an SNMP trap when an illegal MAC address is detected on an Ethernet hub port, use the following commands in hub configuration mode.

	Command	Purpose
Step 1	`Router(config-hub)# hub ethernet number port [end-port]`	Specifies the hub number and the hub port (or range of hub ports) and enters hub configuration mode.
Step 2	`Router(config-hub)# snmp trap illegal-address`	Enables the router to issue an SNMP trap when an illegal MAC address is detected on the hub port.

You may need to set up a host receiver for this trap type (snmp-server host) for a Network Management System (NMS) to receive this trap type. The default is no trap. For an example of configuring a SNMP trap for an Ethernet hub port, see the "Hub Configuration Examples" section on page 71.

Configuring a Token Ring Interface

Cisco supports various Token Ring interfaces. Refer to the *Cisco Product Catalog* for information about platform and hardware compatibility.

The Token Ring interface supports both routing (Layer 3 switching) and source-route bridging (Layer 2 switching) on a per-protocol basis. For example, IP traffic could be routed, while SNA traffic is bridged. Routing features enhance source-route bridges

The Token Ring MIB variables support the specification in RFC 1231, *IEEE 802.5 Token Ring MIB*. The mandatory Interface Table and Statistics Table are implemented, but the optional Timer Table of the Token Ring MIB is not. The Token Ring MIB has been implemented for the Token Ring Interface Processor (TRIP).

Use the **show interfaces**, **show controllers token**, and **show controllers cbus** EXEC commands to display the Token Ring numbers. These commands provide a report for each ring that Cisco IOS software supports.

Note If the system receives an indication of a cabling problem from a Token Ring interface, it puts that interface into a reset state and does not attempt to restart it. It functions this way because periodic attempts to restart the Token Ring interface drastically affect the stability of routing tables. Once you have plugged the cable into the MAU (media attachment unit) again, restart the interface by using the **clear interface tokenring** *number* command, where the *number* argument is the interface number.

By default, the Token Ring interface uses the SNAP encapsulation format defined in RFC 1042. It is not necessary to define an encapsulation method for this interface.

Particle-Based Switching of Source-Route Bridge Packets on Cisco 7200 Series Routers

Particle-based switching is supported for SRB packets (over FDDI and Token Ring) by default.

Particle-based switching adds scatter-gather capability to SRB to improve performance. Particles represent a communications data packet as a collection of noncontiguous buffers. The traditional Cisco IOS packet has a packet type control structure and a single contiguous data buffer. A particle packet has the same packet type control structure, but it also maintains a queue of particle type structures, each of which manages its own block.

The scatter-gather architecture used by particle-based switching provides the following advantages:

- Allows drivers to use memory more efficiently (especially when using media that has a large maximum transmission unit [MTU]). For example, Token Ring buffers could be 512 bytes rather than 16 KB.
- Allows concurrent use of the same region of memory. For example, on IP multicast a single packet is received and sent out on multiple interfaces simultaneously.
- Allows insertion or deletion of memory at any location in a packet (not just at the beginning or end).

For information about configuring SRB over FDDI, refer to the “Configuring Source-Route Bridging” chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

Dedicated Token Ring Port Adapter

The Dedicated Token Ring port adapter (PA-4R-DTR) is available on Cisco 7500 series routers, Cisco 7200 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

The PA-4R-DTR provides up to four IBM Token Ring or IEEE 802.5 Token Ring interfaces. Each Token Ring interface can be set for 4-Mbps or 16-Mbps half-duplex or full-duplex operation and can operate as a standard Token Ring station or as a concentrator port. The default for all interfaces is Token Ring station mode with half-duplex 16-Mbps operation. The PA-4R-DTR connects over Type 1 lobe or Type 3 lobe cables, with each interface providing an RJ-45 receptacle.

Token Ring Interface Configuration Task List

To configure a Token Ring interface, perform the tasks in the following sections. Each task is identified as either required or optional.

- Specifying a Token Ring Interface, page 65 (Required)
- Enabling Early Token Release, page 65 (Optional)
- Configuring PCbus Token Ring Interface Management, page 65 (Optional)
- Enabling a Token Ring Concentrator Port, page 65 (Optional)
- Monitoring and Maintaining the Port, page 66 (Optional)

Specifying a Token Ring Interface

To specify a Token Ring interface and enter interface configuration mode, use one of the following commands in global configuration mode.

Command	Purpose
`Router(config)#` **`interface tokenring`** *`number`*	Enters interface configuration mode.
`Router(config)#` **`interface tokenring`** *`slot`*/*`port`*	Enters interface configuration mode for the Cisco 7200 or Cisco 7500 series routers.
`Router(config)#` **`interface tokenring`** *`slot`*/*`port-adapter`*/*`port`*	Enters interface configuration mode for the Cisco 7500 series routers.

Enabling Early Token Release

Cisco Token Ring interfaces support early token release, a method whereby the interface releases the token back onto the ring immediately after transmitting rather than waiting for the frame to return. This feature can help to increase the total bandwidth of the Token Ring. To configure the interface for early token release, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`early-token-release`**	Enables early token release.

Configuring PCbus Token Ring Interface Management

The Token Ring interface on the AccessPro PC card can be managed by a remote LAN manager over the PCbus interface. Currently, the LanOptics Hub Networking Management software running on an IBM-compatible PC is supported.

To enable LanOptics Hub Networking Management of a PCbus Token Ring interface, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`local-lnm`**	Enables PCbus LAN management.

Enabling a Token Ring Concentrator Port

To enable an interface to operate as a concentrator port, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`port`**	Specifies concentrator port operation.

Monitoring and Maintaining the Port

To monitor the Token Ring concentrator port, use one or more of the following commands in EXEC mode.

Command	Purpose
`Router# show controllers token`	Displays internal state information about the Token Ring interfaces in the system.
`Router# show interfaces token`	Displays high-level statistics for a particular interface.

LAN Interface Configuration Examples

This section provides the following examples to illustrate configuration tasks described in this chapter.

- Ethernet Encapsulation Enablement Example, page 66
- Full-Duplex Enablement Operation Example, page 66
- PA-12E/2FE Port Configuration Examples, page 67
- PA-VG100 Port Adapter Configuration Example, page 68
- Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Configuration Examples, page 68
- Fast EtherChannel Configuration Examples, page 69
- FDDI Frames Configuration Example, page 70
- Hub Configuration Examples, page 71

Ethernet Encapsulation Enablement Example

These commands enable standard Ethernet Version 2.0 encapsulation on the Ethernet interface processor in slot 4 on port 2 of a Cisco 7500 series router:

```
interface ethernet 4/2
 encapsulation arpa
```

Full-Duplex Enablement Operation Example

The following example assigns an IP address and subnet mask, specifies an MII Ethernet connector, and enables full-duplex mode on Fast Ethernet interface port 0 in slot 1 port adapter 0:

```
Router(config)# interface fastethernet 1/0/0
Router(config-if)# ip address 10.1.1.10 255.255.255.0
Router(config-if)# full-duplex
Router(config-if)# media-type mii
Router(config-if)# exit
Router(config)# exit
```

PA-12E/2FE Port Configuration Examples

The following is an example of a configuration for the PA-12E/2FE port adapter interface. Bridge groups 10, 20, and 30 use IEEE Spanning Tree Protocol. The first four interfaces of a PA-12E/2EF port adapter in port adapter slot 3 use bridge groups 10 and 20. Each interface is assigned to a bridge group, and the shutdown state is set to up. The PA-12E/2FE port adapter supports store-and-forward or cut-through switching technology between interfaces within the same bridge group; store-and-forward is the default. In the following example, the **cut-through** command is used to configure each interface for cut-through switching of received and transmitted data:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
Router(config)# bridge 10 protocol ieee
Router(config)# bridge 20 protocol ieee
Router(config)# bridge 30 protocol ieee

Router(config)# interface fastethernet 3/0
Router(config-if)# bridge-group 10
Router(config-if)# cut-through
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Fast Ethernet3/0, changed
state to up
%LINK-3-UPDOWN: Interface Fast Ethernet3/0, changed state to up

Router(config)# interface fastethernet 3/1
Router(config-if)# bridge-group 10
Router(config-if)# cut-through
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Fast Ethernet3/1, changed
state to up
%LINK-3-UPDOWN: Interface Fast Ethernet3/1, changed state to up

Router(config)# interface ethernet 3/2
Router(config-if)# bridge-group 20
Router(config-if)# cut-through
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/2, changed state to up
%LINK-3-UPDOWN: Interface Ethernet3/2, changed state to up

Router(config)# interface ethernet 3/3
Router(config-if)# bridge-group 20
Router(config-if)# cut-through
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/3, changed state to up
%LINK-3-UPDOWN: Interface Ethernet3/3, changed state to up
```

The following example shows integrated routing and bridging enabled on the bridge groups. Bridge group 10 is assigned an IP address and subnet mask, and the shutdown state is changed to up. Bridge group 10 is configured to route IP.

```
Router(config)# bridge irb
Router(config)# interface bvi 10
Router(config-if)# ip address 10.1.15.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface BVI10, changed state to up

Router(config)# bridge 10 route ip
Router(config)# exit
Router#
```

PA-VG100 Port Adapter Configuration Example

The following is an example of a basic configuration for the PA-VG100 port adapter interface in slot 1 on a Cisco 7500 series router. In this example, IP routing is enabled on the router, so an IP address and subnet mask are assigned to the interface.

```
configure terminal
interface vg-anylan 1/0/0
 ip address 10.1.1.10 255.255.255.0
 no shutdown
 exit
exit
```

Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Configuration Examples

This section provides the following configuration examples:

- Configuring the Gigabit Ethernet Interface on the Cisco 7200-I/O-GE+E, page 68
- Configuring Autonegotiation on the Cisco 7200-I/O-2FE/E, page 69

Configuring the Gigabit Ethernet Interface on the Cisco 7200-I/O-GE+E

The following example configures the Gigabit Ethernet interface on the Cisco 7200-I/O-GE+E. The following commands are configured on slot 0, port 0.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 0/0
Router(config-if)# ip address 10.1.1.10 255.255.255.252
Router(config-if)# negotiation auto
Router(config-if)# end
```

Configuring Autonegotiation on the Cisco 7200-I/O-2FE/E

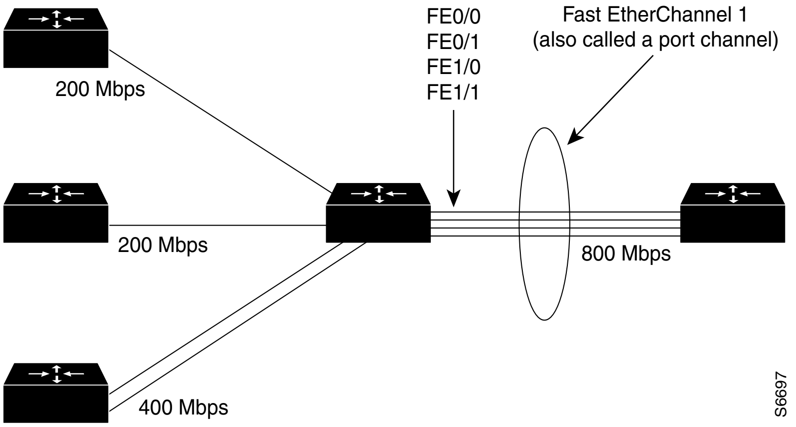
The following example configures the Fast Ethernet interface on the Cisco 7200-I/O-2FE/E for fully enabled autonegotiation:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 0/0
Router(config-if)# duplex auto
Router(config-if)# speed auto
```

Fast EtherChannel Configuration Examples

Figure 3 shows four point-to-point Fast Ethernet interfaces that are aggregated into a single Fast EtherChannel interface.

Figure 3 Fast Ethernet Interfaces Aggregated into a Fast EtherChannel



The configuration file that illustrates this topology follows.

The following is an example of how to create a Fast EtherChannel (port-channel interface) with four Fast Ethernet interfaces. In this example, ISL is enabled on the Fast EtherChannel, and an IP address is assigned to the subinterface.

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface port-channel 1.1
Router(config-if)# ip address 10.1.1.10 255.255.255.0
Router(config-if)# encapsulation isl 100
Router(config-if)# exit
Router(config)# interface fastethernet 0/0/0
Router(config-if)# no ip address
Router(config-if)# channel-group 1
Fast Ethernet 0/0 added as member-1 to port-channel1.
Router(config-if)# exit
Router(config)# interface fastethernet 0/1/0
Router(config-if)# no ip address
Router(config-if)# channel-group 1
Fast Ethernet 0/1 added as member-2 to port-channel1.
Router(config-if)# exit
Router(config)# interface fastethernet 1/0/0
Router(config-if)# no ip address
Router(config-if)# channel-group 1
Fast Ethernet 1/0 added as member-3 to port-channel1.
Router(config-if)# exit
Router(config)# interface fastethernet 1/1/0
Router(config-if)# no ip address
Router(config-if)# channel-group 1
Fast Ethernet 1/1 added as member-4 to port-channel1.
Router(config-if)# exit
Router(config)# exit
Router#
```

The following is a partial example of a configuration file. The MAC address is automatically added to the Fast Ethernet interface when the interfaces are added to the Fast EtherChannel.

Note If you do not assign a static MAC address on the port-channel interface, the Cisco IOS software automatically assigns a MAC address. If you assign a static MAC address and then later remove it, the Cisco IOS software automatically assigns a MAC address.

```
interface Port-channel1
 ip address 10.1.1.10 255.255.255.0
!
interface Port-channel1.1
 encapsulation isl 100
!
interface Fast Ethernet0/0/0
 mac-address 00e0.1476.7600
 no ip address
 channel-group 1
!
interface Fast Ethernet0/1/0
 mac-address 00e0.1476.7600
 no ip address
 channel-group 1
!
interface Fast Ethernet1/0/0
 mac-address 00e0.1476.7600
 no ip address
 channel-group 1
!
interface Fast Ethernet1/1/0
 mac-address 00e0.1476.7600
 no ip address
 channel-group 1
```

FDDI Frames Configuration Example

The following example shows how to configure the FDDI interface to transmit four frames per token capture:

```
! Enter global configuration mode.
  4700# configure terminal
! Enter interface configuration mode.
  4700(config)# interface fddi0
! Show the fddi command options.
  4700(config-if)# fddi ?
  encapsulate             Enable FDDI Encapsulation bridging
  frames-per-token        Maximum frames to transmit per service opportunity
  tl-min-time             Line state transmission time
  token-rotation-time      Set the token rotation timer
  valid-transmission-time  Set transmission valid timer
! Show fddi frames-per-token command options.
  4700(config-if)# fddi frames-per-token ?
  <1-10> Number of frames per token, default = 3
! Specify 4 as the maximum number of frames to be transmitted per token.
  4700(config-if)# fddi frames-per-token 4
```

Hub Configuration Examples

This section provides the following hub configuration examples:

- Hub Port Startup Examples, page 71
- Source Address for an Ethernet Hub Port Configuration Examples, page 71
- Hub Port Shutdown Examples, page 71
- SNMP Illegal Address Trap Enablement for Hub Port Example, page 72

Hub Port Startup Examples

The following example configures port 1 on hub 0 of Ethernet interface 0:

```
hub ethernet 0 1
 no shutdown
```

The following example configures ports 1 through 8 on hub 0 of Ethernet interface 0:

```
hub ethernet 0 1 8
 no shutdown
```

Source Address for an Ethernet Hub Port Configuration Examples

The following example configures the hub to allow only packets from MAC address 1111.2222.3333 on port 2 of hub 0:

```
hub ethernet 0 2
 source-address 1111.2222.3333
```

The following example configures the hub to remember the first MAC address received on port 2 and allow only packets from that learned MAC address:

```
hub ethernet 0 2
 source-address
```

Hub Port Shutdown Examples

The following example shuts down ports 3 through 5 on hub 0:

```
hub ethernet 0 3 5
 shutdown
```

The following example shuts down port 3 on hub 0:

```
hub ethernet 0 3
 shutdown
```

SNMP Illegal Address Trap Enablement for Hub Port Example

The following example specifies the gateway IP address and enables an SNMP trap to be issued to the host 172.16.40.51 when a MAC address violation is detected on hub ports 2, 3, or 4. It specifies that Ethernet interface 0 is the source for all traps on the router. The community string is defined as the string *public* and the read/write parameter is set.

```
ip route 0.0.0.0 0.0.0.0 172.22.10.1
snmp-server community public rw
snmp-server trap-source ethernet 0
snmp-server host 172.16.40.51 public
hub ethernet 0 2 4
snmp trap illegal-address
```

EtherSwitch Network Module

This document explains how to configure the EtherSwitch network module. This network module is supported on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. The EtherSwitch network module is a modular, high-density voice network module that provides Layer 2 switching across Ethernet ports. The EtherSwitch network module has sixteen 10/100 switched Ethernet ports with integrated inline power and QoS features that are designed to extend Cisco AVVID-based voice-over-IP (VoIP) networks to small branch offices.

Feature History for the EtherSwitch Module Feature

Release	Modification
12.2(2)XT	This feature was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)ZJ	Added switching software enhancements: IEEE 802.1x, QoS (including Layer 2/Layer 3 CoS/DSCP mapping and rate limiting), security ACL, IGMP snooping, per-port storm control, and fallback bridging support for switch virtual interfaces (SVIs).
12.3(4)T	The switching software enhancements from Cisco IOS Release 12.2(15)ZJ were integrated into Cisco IOS Release 12.3(4)T.

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 the EtherSwitch Network Module

- Cisco IOS Release 12.3 or later release
- Basic configuration of the Cisco 2600 series, Cisco 3600 series, or Cisco 3700 series router

In addition, complete the following tasks before configuring this feature:

- Configure IP routing

  For more information on IP routing, refer to the *Cisco IOS IP Configuration Guide*.
- Set up the call agents

  For more information on setting up call agents, refer to the documentation that accompanies the call agents used in your network configuration.

Restrictions for the EtherSwitch Network Module

The following functions are not supported by the EtherSwitch network module:

- CGMP client, CGMP fast-leave
- Dynamic ports
- Dynamic access ports
- Secure ports
- Dynamic trunk protocol
- Dynamic VLANs
- GARP, GMRP, and GVRP
- ISL tagging (The chip does not support ISL.)
- Layer 3 switching onboard
- Monitoring of VLANs
- Multi-VLAN ports Network Port
- Shared STP instances
- STP uplink fast for clusters
- VLAN-based SPAN
- VLAN Query Protocol
- VTP Pruning Protocol
- Web-based management interface

Information About the EtherSwitch Network Module

To configure the EtherSwitch network module, you should understand the following concepts:

EtherSwitch Network Module: Benefits

- Statistical gains by combining multiple traffic types over a common IP infrastructure.
- Long distance savings
- Support for intra-chassis stacking
- Voice connectivity over data applications
- IPSec, ACL, VPN and Firewall options
- New broadband WAN options

The Interface Range Specification feature makes configuration easier for these reasons:

- Identical commands can be entered once for a range of interfaces, rather than being entered separately for each interface.
- Interface ranges can be saved as macros.

Ethernet Switching in Cisco AVVID Architecture

The EtherSwitch network module is designed to work as part of the Cisco Architecture for Voice, Video, and Integrated Data (AVVID) solution. The EtherSwitch network module has sixteen 10/100 switched Ethernet ports with integrated inline power and QoS features that allow for extending Cisco AVVID-based voice-over-IP (VoIP) networks to small branch offices.

The 16-port EtherSwitch network module has sixteen 10/100BASE-TX ports and an optional 10/100/1000BASE-T Gigabit Ethernet port. The 36-port EtherSwitch network module has thirty six 10/100BASE-TX ports and two optional 10/100/1000BASE-T Gigabit Ethernet ports. The gigabit Ethernet can be used as an uplink port to a server or as a stacking link to another 16- or 36-port EtherSwitch network module in the same system. The 36-port EtherSwitch network module requires a double-wide slot. An optional power module can also be added to provide inline power for IP telephones.

As an access gateway switch, the EtherSwitch network module can be deployed as a component of a centralized call-processing network using a centrally deployed Cisco CallManager (CCM). Instead of deploying and managing key systems or PBXs in small branch offices, applications are centrally located at the corporate headquarters or data center and are accessed via the IP WAN.

By default, the EtherSwitch network module provides the following settings with respect to Cisco AVVID:

- All switch ports are in access VLAN 1.
- All switch ports are static access ports, not 802.1Q trunk ports.
- Default voice VLAN is not configured on the switch.
- Inline power is automatically supplied on the 10/100 ports.

VLANs

Virtual local-area networks (VLANs) are a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLAN Trunk Protocol

VLAN Trunk Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more switches that share the same VTP domain name and that are interconnected with trunks. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations. Before you create VLANs, you must decide whether to use VTP in your network. With VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network.

VTP Domain

A VTP domain (also called a VLAN management domain) is made up of one or more interconnected switches that share the same VTP domain name. A switch can be configured to be in only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

By default, the switch is in VTP server mode and is in an un-named domain state until the switch receives an advertisement for a domain over a trunk link or until you configure a management domain. You cannot create or modify VLANs on a VTP server until the management domain name is specified or learned.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch ignores advertisements with a different management domain name or an earlier configuration revision number.

If you configure the switch as VTP transparent, you can create and modify VLANs, but the changes affect only the individual switch.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are transmitted out all trunk connections using IEEE 802.1Q encapsulation.

VTP maps VLANs dynamically across multiple LAN types with unique names and internal index associations. Mapping eliminates excessive device administration required from network administrators.

VTP Modes

You can configure a switch to operate in any one of these VTP modes:

- Server—In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.
- Client—VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
- Transparent—VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive out their trunk interfaces.

VTP Advertisements

Each switch in the VTP domain sends periodic advertisements out each trunk interface to a reserved multicast address. VTP advertisements are received by neighboring switches, which update their VTP and VLAN configurations as necessary.

The following global configuration information is distributed in VTP advertisements:

- VLAN IDs (801.Q)
- VTP domain name
- VTP configuration revision number
- VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
- Frame format

VTP Version 2

If you use VTP in your network, you must decide whether to use VTP version 1 or version 2. VTP version 2 supports the following features not supported in version 1:

Unrecognized Type-Length-Value (TLV) Support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM.

Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version, and forwards a message only if the version and domain name match. Since only one domain is supported in the NM-16ESW software, VTP version 2 forwards VTP messages in transparent mode, without checking the version.

Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message, or when information is read from NVRAM. If the digest on a received VTP message is correct, its information is accepted without consistency checks.

VTP Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when implementing VTP in your network:

- All switches in a VTP domain must run the same VTP version.
- You must configure a password on each switch in the management domain when in secure mode.
- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1, provided that VTP version 2 is disabled on the VTP version 2-capable switch. (VTP version 2 is disabled by default).
- Do not enable VTP version 2 on a switch unless all switches in the same VTP domain are version 2-capable. When you enable VTP version 2 on a switch, all version 2-capable switches in the domain enable VTP version 2.
- The Cisco IOS **end** command and the **Ctrl-Z** keystrokes are not supported in VLAN database mode.
- The VLAN database stored on internal Flash is supported.
- Use the **squeeze flash** command to remove old copies of overwritten VLAN databases.

Inline Power for Cisco IP Phones

The EtherSwitch network module can supply inline power to a Cisco 7960 IP phone, if required. The Cisco 7960 IP phone can also be connected to an AC power source and supply its own power to the voice circuit. When the Cisco 7960 IP phone is supplying its own power, a EtherSwitch network module can forward IP voice traffic to and from the phone.

A detection mechanism on the EtherSwitch network module determines whether it is connected to a Cisco 7960 IP phone. If the switch senses that there is *no* power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch to never supply power to the Cisco 7960 IP phone and to disable the detection mechanism.

Using the Spanning Tree Protocol with the EtherSwitch network module

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or to a switched LAN of multiple segments.

The EtherSwitch network module uses STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided that you do not manually disable STP). You can enable and disable STP on a per-VLAN basis.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The spanning tree algorithm calculates the best loop-free path throughout a switched Layer 2 network. Switches send and receive spanning tree frames at regular intervals. The switches do not forward these frames but use the frames to construct a loop-free path.

Multiple active paths between end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages and switches might learn endstation MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network.

Spanning Tree Protocol (STP) defines a tree with a root switch and a loop-free path from the root to all switches in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning tree algorithm recalculates the spanning tree topology and activates the standby path.

When two ports on a switch are part of a loop, the spanning tree port priority and port path cost setting determine which port is put in the forwarding state and which port is put in the blocking state. The spanning tree port priority value represents the location of an interface in the network topology and how well located it is to pass traffic. The spanning tree port path cost value represents media speed.

Bridge Protocol Data Units

The stable active spanning tree topology of a switched network is determined by the following:

- The unique bridge ID (bridge priority and MAC address) associated with each VLAN on each switch
- The spanning tree path cost to the root bridge
- The port identifier (port priority and MAC address) associated with each Layer 2 interface

The Bridge Protocol Data Units (BPDU) are transmitted in one direction from the root switch, and each switch sends configuration BPDUs to communicate and compute the spanning tree topology. Each configuration BPDU contains the following minimal information:

- The unique bridge ID of the switch that the transmitting switch believes to be the root switch
- The spanning tree path cost to the root
- The bridge ID of the transmitting bridge
- Message age
- The identifier of the transmitting port
- Values for the hello, forward delay, and max-age protocol timers

When a switch transmits a BPDU frame, all switches connected to the LAN on which the frame is transmitted receive the BPDU. When a switch receives a BPDU, it does not forward the frame but instead uses the information in the frame to calculate a BPDU, and, if the topology changes, initiate a BPDU transmission.

A BPDU exchange results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch based on the path cost.
- A designated bridge for each LAN segment is selected. This is the switch closest to the root bridge through which frames are forwarded to the root.
- A root port is selected. This is the port providing the best path from the bridge to the root bridge.
- Ports included in the spanning tree are selected.
- The Root Bridge is elected.

For each VLAN, the switch with the highest bridge priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch.

The spanning tree root switch is the logical center of the spanning tree topology in a switched network. All paths that are not needed to reach the root switch from anywhere in the switched network are placed in spanning tree blocking mode.

BPDUs contain information about the transmitting bridge and its ports, including bridge and MAC addresses, bridge priority, port priority, and path cost. Spanning tree uses this information to elect the root bridge and root port for the switched network, as well as the root port and designated port for each switched segment.

STP Timers

Table 5 describes the STP timers that affect the entire spanning tree performance.

Table 5 STP Timers

Timer	Purpose
Hello timer	Determines how often the switch broadcasts hello messages to other switches.
Forward delay timer	Determines how long each of the listening and learning states will last before the port begins forwarding.
Maximum age timer	Determines the amount of time protocol information received on a port is stored by the switch.

Spanning Tree Port States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When a Layer 2 interface changes directly from nonparticipation in the spanning tree topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for frames that have been forwarded using the old topology.

Each Layer 2 interface on a switch using spanning tree exists in one of the following five states:

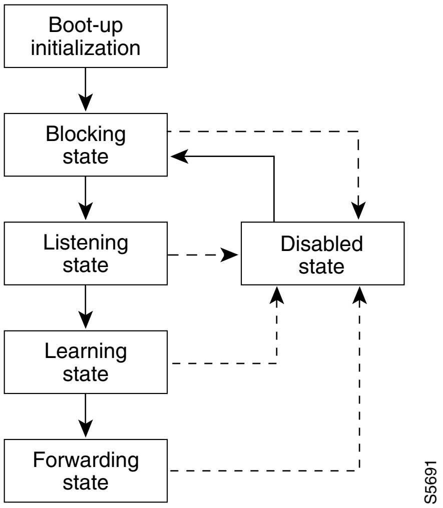
- Blocking—The Layer 2 interface does not participate in frame forwarding.
- Listening—First transitional state after the blocking state when spanning tree determines that the Layer 2 interface should participate in frame forwarding.
- Learning—The Layer 2 interface prepares to participate in frame forwarding.
- Forwarding—The Layer 2 interface forwards frames.
- Disabled—The Layer 2 interface does not participate in spanning tree and is not forwarding frames.

A Layer 2 interface moves through these five states as follows:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

Figure 4 illustrates how a port moves through the five stages.

Figure 4 STP Port States



Boot-up Initialization

When you enable spanning tree, every port in the switch, VLAN, or network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, each Layer 2 interface stabilizes to the forwarding or blocking state.

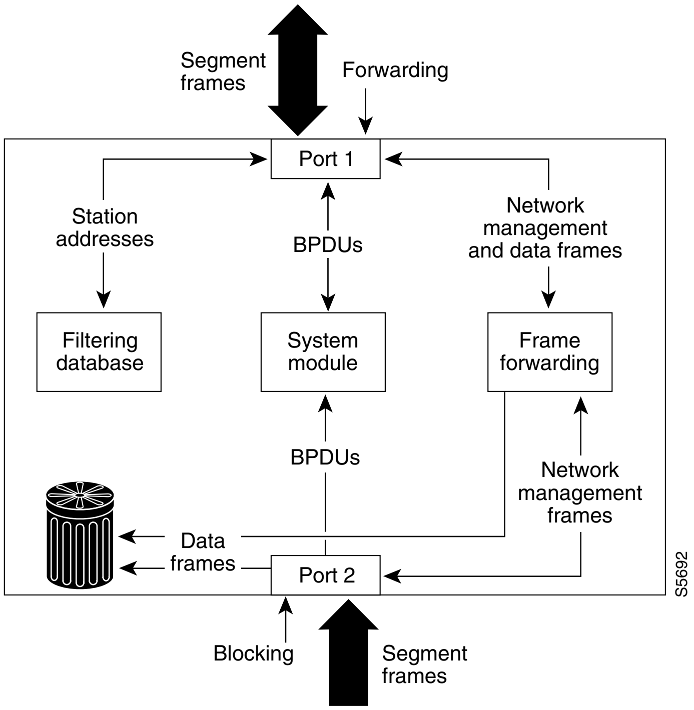
When the spanning tree algorithm places a Layer 2 interface in the forwarding state, the following process occurs:

1. The Layer 2 interface is put into the listening state while it waits for protocol information that suggests that it should go to the blocking state.
2. The Layer 2 interface waits for the forward delay timer to expire, moves the Layer 2 interface to the learning state, and resets the forward delay timer.
3. In the learning state, the Layer 2 interface continues to block frame forwarding as it learns end station location information for the forwarding database.
4. The Layer 2 interface waits for the forward delay timer to expire and then moves the Layer 2 interface to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A Layer 2 interface in the blocking state does not participate in frame forwarding, as shown in Figure 5. After initialization, a BPDU is sent out to each Layer 2 interface in the switch. A switch initially assumes it is the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root bridge. If only one switch is in the network, no exchange occurs, the forward delay timer expires, and the ports move to the listening state. A port always enters the blocking state following switch initialization.

Figure 5 Interface 2 in Blocking State



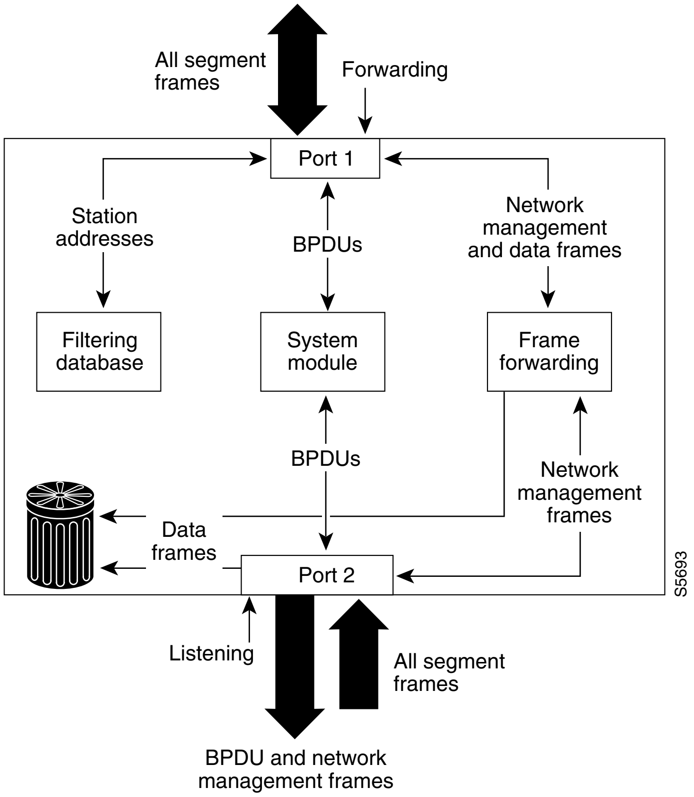
A Layer 2 interface in the blocking state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another interface for forwarding.
- Does not incorporate end station location into its address database. (There is no learning on a blocking Layer 2 interface, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Does not transmit BPDUs received from the system module.
- Receives and responds to network management messages.

Listening State

The listening state is the first transitional state a Layer 2 interface enters after the blocking state. The Layer 2 interface enters this state when STP determines that the Layer 2 interface should participate in frame forwarding. Figure 6 shows a Layer 2 interface in the listening state.

Figure 6 Interface 2 in Listening State



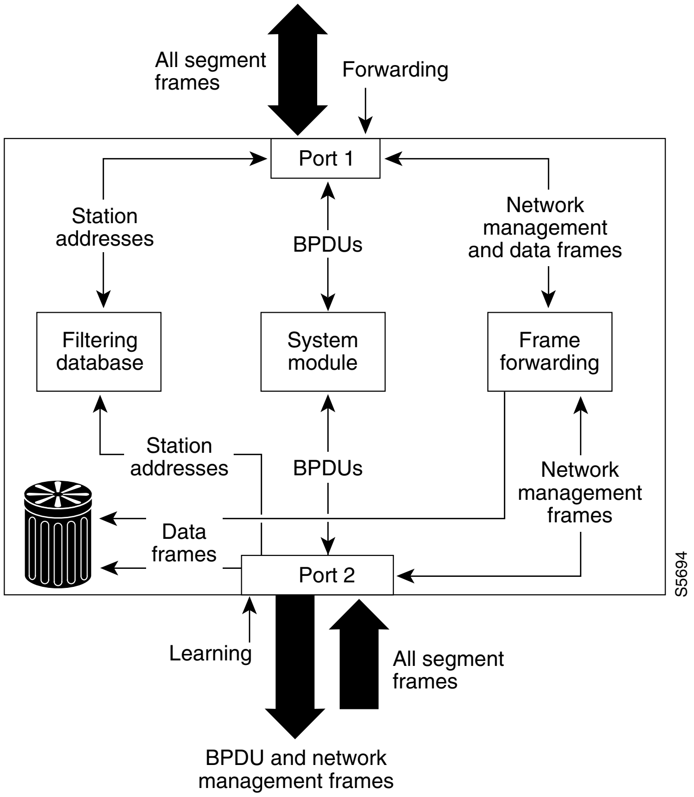
A Layer 2 interface in the listening state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another interface for forwarding.
- Does not incorporate end station location into its address database. (There is no learning at this point, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Learning State

A Layer 2 interface in the learning state prepares to participate in frame forwarding. The Layer 2 interface enters the learning state from the listening state. Figure 7 shows a Layer 2 interface in the learning state.

Figure 7 Interface 2 in Learning State



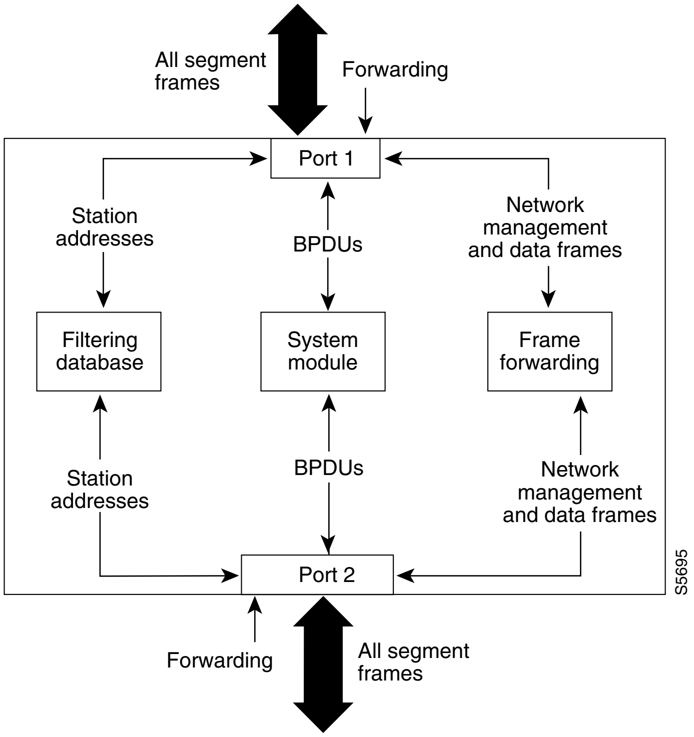
A Layer 2 interface in the learning state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another interface for forwarding.
- Incorporates end station location into its address database.
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Forwarding State

A Layer 2 interface in the forwarding state forwards frames, as shown in Figure 8. The Layer 2 interface enters the forwarding state from the learning state.

Figure 8 Interface 2 in Forwarding State



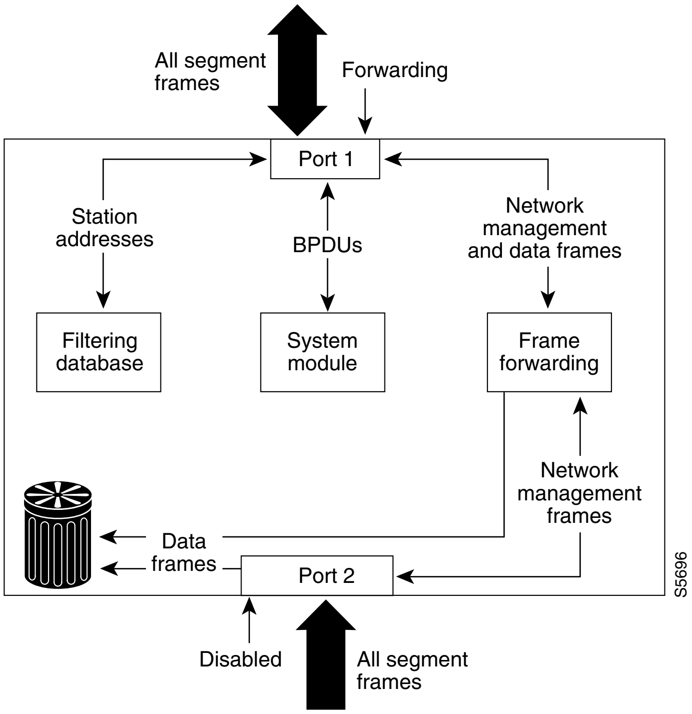
A Layer 2 interface in the forwarding state performs as follows:

- Forwards frames received from the attached segment.
- Forwards frames switched from another Layer 2 interface for forwarding.
- Incorporates end station location information into its address database.
- Receives BPDUs and directs them to the system module.
- Processes BPDUs received from the system module.
- Receives and responds to network management messages.

Disabled State

A Layer 2 interface in the disabled state does not participate in frame forwarding or spanning tree, as shown in Figure 9. A Layer 2 interface in the disabled state is virtually nonoperational.

Figure 9 Interface 2 in Disabled State



A disabled Layer 2 interface performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another Layer 2 interface for forwarding.
- Does not incorporate end station location into its address database. (There is no learning, so there is no address database update.)
- Does not receive BPDUs.
- Does not receive BPDUs for transmission from the system module.

MAC Address Allocation

The MAC address allocation manager has a pool of MAC addresses that are used as the bridge IDs for the VLAN spanning trees. In Table 6 you can view the number of VLANs allowed for each platform.

Table 6 Number of VLANs Allowed by Platform

Platform	Maximum Number of VLANs Allowed
Cisco 3640 or higher	64 VLANs
Cisco 2600	32 VLANs

MAC addresses are allocated sequentially, with the first MAC address in the range assigned to VLAN 1, the second MAC address in the range assigned to VLAN 2, and so forth.

For example, if the MAC address range is 00-e0-1e-9b-2e-00 to 00-e0-1e-9b-31-ff, the VLAN 1 bridge ID is 00-e0-1e-9b-2e-00, the VLAN 2 bridge ID is 00-e0-1e-9b-2e-01, the VLAN 3 bridge ID is 00-e0-1e-9b-2e-02, and so forth.

Default Spanning Tree Configuration

Table 7 shows the default Spanning Tree configuration values.

Table 7 Spanning Tree Default Configuration

Feature	Default Value
Enable state	Spanning tree enabled for all VLANs
Bridge priority	32768
Spanning tree port priority (configurable on a per-interface basis; used on interfaces configured as Layer 2 access ports)	128
Spanning tree port cost (configurable on a per-interface basis; used on interfaces configured as Layer 2 access ports)	Fast Ethernet: 19 Ethernet: 100 Gigabit Ethernet: 19 when operated in 100-Mb mode, and 4 when operated in 1000-Mb mode
Spanning tree VLAN port priority (configurable on a per-VLAN basis; used on interfaces configured as Layer 2 trunk ports)	128
Spanning tree VLAN port cost (configurable on a per-VLAN basis; used on interfaces configured as Layer 2 trunk ports)	Fast Ethernet: 10 Ethernet: 10
Hello time	2 seconds
Forward delay time	15 seconds
Maximum aging time	20 seconds

Spanning Tree Port Priority

In the event of a loop, spanning tree considers port priority when selecting an interface to put into the forwarding state. You can assign higher priority values to interfaces that you want spanning tree to select first, and lower priority values to interfaces that you want spanning tree to select last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks other interfaces. The possible priority range is 0 to 255, configurable in increments of 4 (the default is 128).

Cisco IOS software uses the port priority value when the interface is configured as an access port and uses VLAN port priority values when the interface is configured as a trunk port.

Spanning Tree Port Cost

The spanning tree port path cost default value is derived from the media speed of an interface. In the event of a loop, spanning tree considers port cost when selecting an interface to put into the forwarding state. You can assign lower cost values to interfaces that you want spanning tree to select first and higher cost values to interfaces that you want spanning tree to select last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

The possible cost range is 0 to 65535 (the default is media-specific).

Spanning tree uses the port cost value when the interface is configured as an access port and uses VLAN port cost values when the interface is configured as a trunk port.

BackboneFast

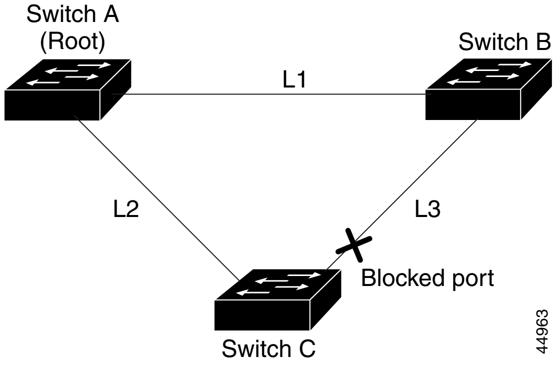
BackboneFast is initiated when a root port or blocked port on a switch receives inferior BPDUs from its designated bridge. An inferior BPDU identifies one switch as both the root bridge and the designated bridge. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an *indirect* link) has failed (that is, the designated bridge has lost its connection to the root switch). Under STP rules, the switch ignores inferior BPDUs for the configured maximum aging time specified by the **spanning-tree max-age** global configuration command.

The switch tries to determine if it has an alternate path to the root switch. If the inferior BPDU arrives on a blocked port, the root port and other blocked ports on the switch become alternate paths to the root switch. (Self-looped ports are not considered alternate paths to the root switch.) If the inferior BPDU arrives on the root port, all blocked ports become alternate paths to the root switch. If the inferior BPDU arrives on the root port and there are no blocked ports, the switch assumes that it has lost connectivity to the root switch, causes the maximum aging time on the root to expire, and becomes the root switch according to normal STP rules.

If the switch has alternate paths to the root switch, it uses these alternate paths to transmit a new kind of Protocol Data Unit (PDU) called the Root Link Query PDU. The switch sends the Root Link Query PDU on all alternate paths to the root switch. If the switch determines that it still has an alternate path to the root, it causes the maximum aging time on the ports on which it received the inferior BPDU to expire. If all the alternate paths to the root switch indicate that the switch has lost connectivity to the root switch, the switch causes the maximum aging times on the ports on which it received an inferior BPDU to expire. If one or more alternate paths can still connect to the root switch, the switch makes all ports on which it received an inferior BPDU its designated ports and moves them out of the blocking state (if they were in the blocking state), through the listening and learning states, and into the forwarding state.

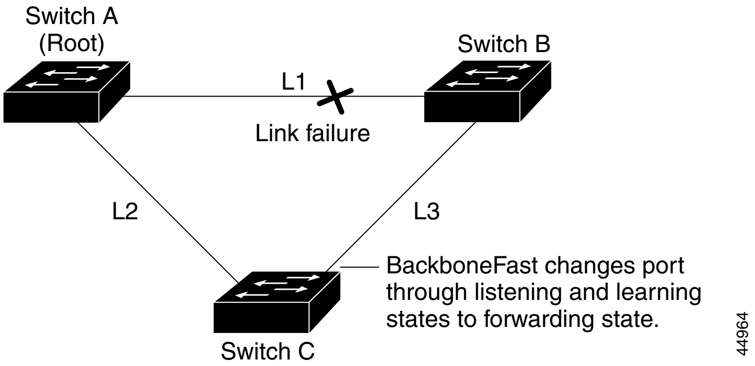
Figure 10 shows an example topology with no link failures. Switch A, the root switch, connects directly to Switch B over link L1 and to Switch C over link L2. The interface on Switch C that connects directly to Switch B is in the blocking state.

Figure 10 BackboneFast Example Before Indirect Link Failure



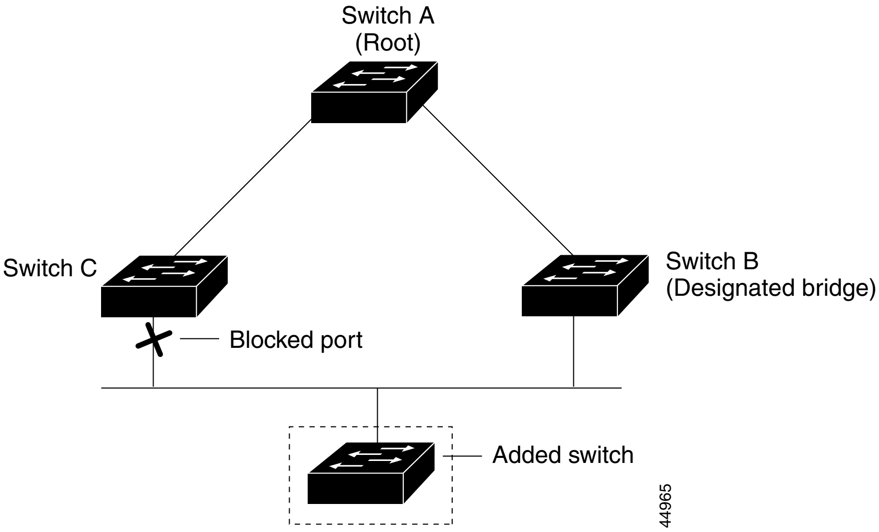
If link L1 fails, Switch C cannot detect this failure because it is not connected directly to link L1. However, because Switch B is directly connected to the root switch over L1, it detects the failure, elects itself the root, and begins sending BPDUs to Switch C, identifying itself as the root. When Switch C receives the inferior BPDUs from Switch B, Switch C assumes that an indirect failure has occurred. At that point, BackboneFast allows the blocked port on Switch C to move immediately to the listening state without waiting for the maximum aging time for the port to expire. BackboneFast then changes the interface on Switch C to the forwarding state, providing a path from Switch B to Switch A. This switchover takes approximately 30 seconds, twice the Forward Delay time if the default Forward Delay time of 15 seconds is set. Figure 11 shows how BackboneFast reconfigures the topology to account for the failure of link L1.

Figure 11 BackboneFast Example After Indirect Link Failure


Switch A
(Root)
Switch B
L1
Link failure
L2
L3
BackboneFast changes port through listening and learning states to forwarding state.
Switch C
44964

If a new switch is introduced into a shared-medium topology as shown in Figure 12, BackboneFast is not activated because the inferior BPDUs did not come from the recognized designated bridge (Switch B). The new switch begins sending inferior BPDUs that say it is the root switch. However, the other switches ignore these inferior BPDUs, and the new switch learns that Switch B is the designated bridge to Switch A, the root switch.

Figure 12 Adding a Switch in a Shared-Medium Topology



Layer 2 Ethernet Switching

EtherSwitch network modules support simultaneous, parallel connections between Layer 2 Ethernet segments. Switched connections between Ethernet segments last only for the duration of the packet. New connections can be made between different segments for the next packet.

The EtherSwitch network module solves congestion problems caused by high-bandwidth devices and a large number of users by assigning each device (for example, a server) to its own 10-, 100-, or 1000-Mbps segment. Because each Ethernet interface on the switch represents a separate Ethernet segment, servers in a properly configured switched environment achieve full access to the bandwidth.

Because collisions are a major bottleneck in Ethernet networks, an effective solution is full-duplex communication. Normally, Ethernet operates in half-duplex mode, which means that stations can either receive or transmit. In full-duplex mode, two stations can transmit and receive at the same time. When packets can flow in both directions simultaneously, effective Ethernet bandwidth doubles to 20 Mbps for 10-Mbps interfaces and to 200 Mbps for Fast Ethernet interfaces.

Switching Frames Between Segments

Each Ethernet interface on an EtherSwitch network module can connect to a single workstation or server, or to a hub through which workstations or servers connect to the network.

On a typical Ethernet hub, all ports connect to a common backplane within the hub, and the bandwidth of the network is shared by all devices attached to the hub. If two stations establish a session that uses a significant level of bandwidth, the network performance of all other stations attached to the hub is degraded.

To reduce degradation, the switch treats each interface as an individual segment. When stations on different interfaces need to communicate, the switch forwards frames from one interface to the other at wire speed to ensure that each session receives full bandwidth.

To switch frames between interfaces efficiently, the switch maintains an address table. When a frame enters the switch, it associates the MAC address of the sending station with the interface on which it was received.

Building the Address Table

The EtherSwitch network module builds the address table by using the source address of the frames received. When the switch receives a frame for a destination address not listed in its address table, it floods the frame to all interfaces of the same virtual local-area network (VLAN) except the interface that received the frame. When the destination station replies, the switch adds its relevant source address and interface ID to the address table. The switch then forwards subsequent frames to a single interface without flooding to all interfaces. The address table can store at least 8,191 address entries without flooding any entries. The switch uses an aging mechanism, defined by a configurable aging timer; so if an address remains inactive for a specified number of seconds, it is removed from the address table.

Note Default parameters on the aging timer are recommended.

VLAN Trunks

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network and supports only one encapsulation on all Ethernet interfaces: 802.1Q-802.1Q is an industry-standard trunking encapsulation. You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle.

Layer 2 Interface Modes

Two Ethernet interface modes can be configured. Using the **switchport** command with the **mode access** keywords puts the interface into nontrunking mode. The interface will stay in access mode regardless of what the connected port mode is. Only access VLAN traffic will travel on the access port and untagged (802.3).

Using the **switchport** command with the **mode trunk** keywords puts the interface into permanent trunking mode.

Table 8 Default Layer 2 Ethernet Interface Configuration

Feature	Default Value
Interface mode	switchport mode access or trunk
Trunk encapsulation	switchport trunk encapsulation dot1q
Allowed VLAN range	VLANs 1-1005
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1
Spanning Tree Protocol (STP)	Enabled for all VLANs
STP port priority	128
STP port cost	100 for 10-Mbps Ethernet interfaces 19 for 10/100-Mbps Fast Ethernet interfaces 19 for Gigabit Ethernet interfaces operated in 100-Mb mode 4 for Gigabit Ethernet interfaces operated in 1000-Mb mode

When you connect a Cisco switch to a device other than a Cisco device through an 802.1Q trunk, the Cisco switch combines the spanning tree instance of the VLAN trunk with the spanning tree instance of the other 802.1Q switch. However, spanning tree information for each VLAN is maintained by Cisco switches separated by a cloud of 802.1Q switches that are not Cisco switches. The 802.1Q cloud separating the Cisco switches that is not Cisco devised, is treated as a single trunk link between the switches.

Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the VLAN on one end of the trunk is different from the VLAN on the other end, spanning tree loops might result. Inconsistencies detected by a Cisco switch mark the line as broken and block traffic for the specific VLAN.

Disabling spanning tree on the VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning tree loops. Cisco recommends that you leave spanning tree enabled on the VLAN of an 802.1Q trunk or that you disable spanning tree on every VLAN in the network. Make sure that your network is loop-free before disabling spanning tree.

Layer 2 Interface Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring Layer 2 interfaces:

In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. 802.1Q switches that are not Cisco switches, maintain only one instance of spanning tree for all VLANs allowed on the trunks.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all LAN and WAN media that support Subnetwork Access Protocol (SNAP). Each CDP-configured device sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain the time-to-live, or hold-time information, which indicates the length of time a receiving device should hold CDP information before discarding it.

Port Security

You can use port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses specified for that port. Alternatively, you can use port security to filter traffic destined to or received from a specific host based on the host MAC address.

802.1x Authentication

This section describes how to configure IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. As LANs extend to hotels, airports, and corporate lobbies, insecure environments could be created.

Understanding 802.1x Port-Based Authentication

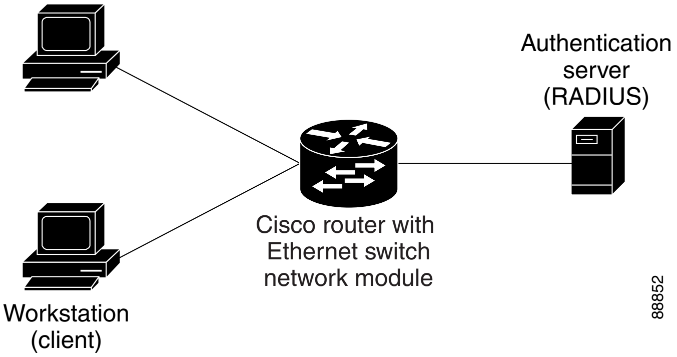
The IEEE 802.1x standard defines a client/server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles as shown in Figure 13.

Figure 13 802.1x Device Roles



- *Client*—the device (workstation) that requests access to the LAN and switch services and responds to the requests from the switch. The workstation must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1x specification.)

Note To resolve Windows XP network connectivity and 802.1x authentication issues, read the Microsoft Knowledge Base article at this URL: http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *Authentication server*—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- *Switch* (edge switch or wireless access point)—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server.

  When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

  The devices that can act as intermediaries include the Catalyst 3550 multilayer switch, Catalyst 2950 switch, or a wireless access point. These devices must be running software that supports the RADIUS client and 802.1x.

Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state changes from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

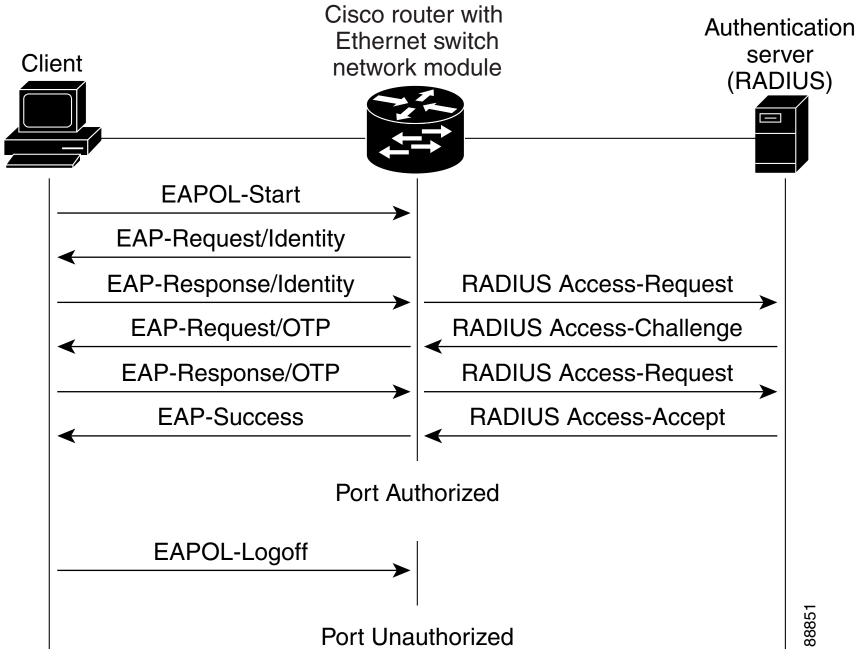
However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

Note If 802.1x is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. Figure 14 shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 14 Message Exchange



Ports in Authorized and Unauthorized States

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1x packets. When a client is successfully authenticated, the port changes to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port that is not running 802.1x, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to change to the unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

Supported Topologies

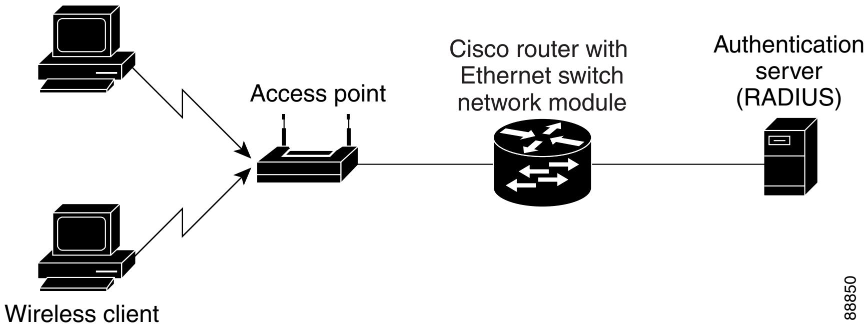
The 802.1x port-based authentication is supported in two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration (see Figure 13 on page 93), only one client can be connected to the 802.1x-enabled switch port. The switch detects the client when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

Figure 15 shows 802.1x-port-based authentication in a wireless LAN. The 802.1x port is configured as a multiple-host port that becomes authorized as soon as one client is authenticated. When the port is authorized, all other hosts indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the switch denies access to the network to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and the wireless access point acts as a client to the switch.

Figure 15 Wireless LAN Example



Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a storm. Storm control can be implemented globally or on a per-port basis. Global storm control and per-port storm control cannot be enabled at the same time.

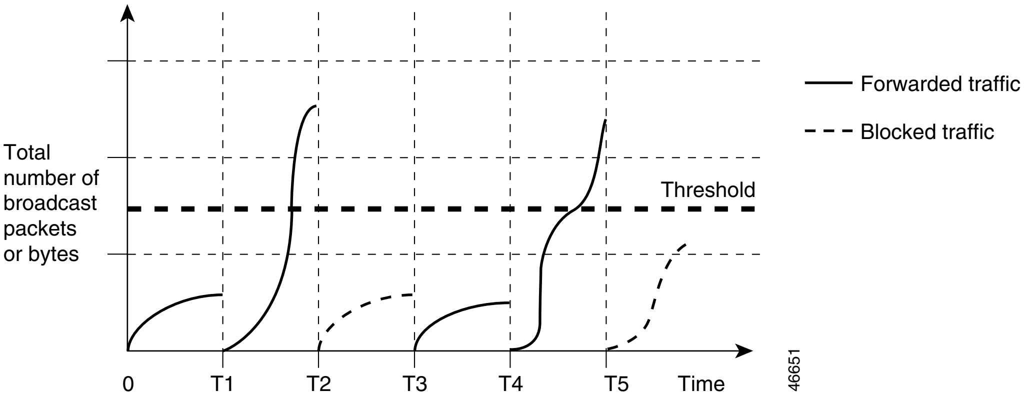
Global Storm Control

Global storm control prevents switchports on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the interfaces. Global storm control monitors incoming traffic statistics over a time period and compares the measurement with a predefined suppression level threshold. The threshold represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level. Global storm control is disabled by default.

The switch supports global storm control for broadcast, multicast, and unicast traffic. This example of broadcast suppression can also be applied to multicast and unicast traffic.

The graph in Figure 16 shows broadcast traffic patterns on an interface over a given period of time. In this example, the broadcast traffic exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped. Therefore, broadcast traffic is blocked during those intervals. At the next time interval, if broadcast traffic does not exceed the threshold, it is again forwarded.

Figure 16 ***Broadcast Suppression Example***



When global storm control is enabled, the switch monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch monitors the number of broadcast, multicast, or unicast packets received within the 1-second time interval, and when a threshold for one type of traffic is reached, that type of traffic is dropped. This threshold is specified as a percentage of total available bandwidth that can be used by broadcast (multicast or unicast) traffic.

The combination of broadcast suppression threshold numbers and the 1-second time interval control the way the suppression algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100 percent means that no limit is placed on the traffic.

Note Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of global storm control.

The switch continues to monitor traffic on the port, and when the utilization level is below the threshold level, the type of traffic that was dropped is forwarded again.

Per-Port Storm Control

A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. By default, per-port storm control is disabled.

Per-port storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

Per-port storm control uses a bandwidth-based method to measure traffic activity. The thresholds are expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic.

The rising threshold is the percentage of total available bandwidth associated with multicast, broadcast, or unicast traffic before forwarding is blocked. The falling threshold is the percentage of total available bandwidth below which the switch resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

EtherChannel

EtherChannel bundles up to eight individual Ethernet links into a single logical link that provides bandwidth of up to 1600 Mbps (Fast EtherChannel full duplex) between the network module and another switch or host.

An EtherSwitch network module system supports a maximum of six EtherChannels. All interfaces in each EtherChannel must have the same speed duplex and mode.

Load Balancing

EtherChannel balances traffic load across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel load balancing can use MAC addresses or IP addresses; either source or destination or both source and destination. The selected mode applies to all EtherChannels configured on the switch.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going only to a single MAC address, using the destination MAC address always chooses the same link in the channel; using source addresses or IP addresses may result in better load balancing.

EtherChannel Configuration Guidelines and Restrictions

If improperly configured, some EtherChannel interfaces are disabled automatically to avoid network loops and other problems. Follow these guidelines and restrictions to avoid configuration problems:

- All Ethernet interfaces on all modules support EtherChannel (maximum of eight interfaces) with no requirement that interfaces be physically contiguous or on the same module.
- Configure all interfaces in an EtherChannel to operate at the same speed and duplex mode.
- Enable all interfaces in an EtherChannel. If you shut down an interface in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining interfaces in the EtherChannel.
- An EtherChannel will not form if one of the interfaces is a Switched Port Analyzer (SPAN) destination port.

For Layer 2 EtherChannels:

- Assign all interfaces in the EtherChannel to the same VLAN, or configure them as trunks.

An EtherChannel supports the same allowed range of VLANs on all interfaces in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the interfaces do not form an EtherChannel.

Interfaces with different Spanning Tree Protocol (STP) port path costs can form an EtherChannel as long they are otherwise compatibly configured. Setting different STP port path costs does not, by itself, make interfaces incompatible for the formation of an EtherChannel.

After you configure an EtherChannel, configuration that you apply to the port-channel interface affects the EtherChannel.

Flow Control on Gigabit Ethernet Ports

Flow control is a feature that Gigabit Ethernet ports use to inhibit the transmission of incoming packets. If a buffer on a Gigabit Ethernet port runs out of space, the port transmits a special packet that requests remote ports to delay sending packets for a period of time. This special packet is called a *pause frame*. The **send** and **receive** keywords of the **set port flowcontrol** command are used to specify the behavior of the pause frames.

Intrachassis Stacking

Multiple switch modules may be installed simultaneously by connecting the Gigabit Ethernet (GE) ports of the EtherSwitch network module. This connection sustains a line-rate traffic similar to the switch fabric found in Cisco Catalyst switches and forms a single VLAN consisting of all ports in multiple EtherSwitch network modules. The stacking port must be configured for multiple switch modules to operate correctly in the same chassis.

- MAC address entries learned via intrachassis stacking are not displayed.
- Link status of intrachassis stacked ports are filtered.

Switched Port Analyzer

Switched Port Analyzer Session

A Switched Port Analyzer (SPAN) session is an association of a destination interface with a set of source interfaces. You configure SPAN sessions using parameters that specify the type of network traffic to monitor. SPAN sessions allow you to monitor traffic on one or more interfaces and to send either ingress traffic, egress traffic, or both to one destination interface. You can configure one SPAN session with separate or overlapping sets of SPAN source interfaces or VLANs. Only switched interfaces can be configured as SPAN sources or destinations on the same network module.

SPAN sessions do not interfere with the normal operation of the switch. You can enable or disable SPAN sessions with command-line interface (CLI) or SNMP commands. When enabled, a SPAN session might become active or inactive based on various events or actions, and this would be indicated by a syslog message. The **show monitor session** command displays the operational status of a SPAN session.

A SPAN session remains inactive after system power-up until the destination interface is operational.

Destination Interface

A destination interface (also called a monitor interface) is a switched interface to which SPAN sends packets for analysis. You can have one SPAN destination interface. Once an interface becomes an active destination interface, incoming traffic is disabled. You cannot configure a SPAN destination interface to receive ingress traffic. The interface does not forward any traffic except that required for the SPAN session.

An interface configured as a destination interface cannot be configured as a source interface. EtherChannel interfaces cannot be SPAN destination interfaces.

Specifying a trunk interface as a SPAN destination interface stops trunking on the interface.

Source Interface

A source interface is an interface monitored for network traffic analysis. One or more source interfaces can be monitored in a single SPAN session with user-specified traffic types (ingress, egress, or both) applicable for all the source interfaces.

You can configure source interfaces in any VLAN. You can configure EtherChannel as source interfaces, which means that all interfaces in the specified VLANs are source interfaces for the SPAN session.

Trunk interfaces can be configured as source interfaces and mixed with nontrunk source interfaces; however, the destination interface never encapsulates.

Traffic Types

Ingress SPAN (Rx) copies network traffic received by the source interfaces for analysis at the destination interface. Egress SPAN (Tx) copies network traffic transmitted from the source interfaces. Specifying the configuration option **both** copies network traffic received and transmitted by the source interfaces to the destination interface.

SPAN Traffic

Network traffic, including multicast, can be monitored using SPAN. Multicast packet monitoring is enabled by default. In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination interface. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination interface d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination interface d1; both packets would be the same (unless a Layer-3 rewrite had occurred, in which case the packets would be different).

Note Monitoring of VLANs is not supported.

SPAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring SPAN:

- Enter the **no monitor session** *session number* command with no other parameters to clear the SPAN session number.
- EtherChannel interfaces can be SPAN source interfaces; they cannot be SPAN destination interfaces.
- If you specify multiple SPAN source interfaces, the interfaces can belong to different VLANs.
- Monitoring of VLANs is not supported
- Only one SPAN session may be run at any given time.
- Outgoing CDP and BPDU packets will not be replicated.
- SPAN destinations never participate in any spanning tree instance. SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the SPAN destination are from the SPAN source.
- Use a network analyzer to monitor interfaces.
- You can have one SPAN destination interface.
- You can mix individual source interfaces within a single SPAN session.
- You cannot configure a SPAN destination interface to receive ingress traffic.
- When enabled, SPAN uses any previously entered configuration.
- When you specify source interfaces and do not specify a traffic type (**Tx**, **Rx**, or **both**), **both** is used by default.

Switched Virtual Interface

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging function in the system. Only one SVI can be associated with a VLAN, but it is necessary to configure an SVI for a VLAN only when you wish to route between VLANs, fallback-bridge nonroutable protocols between VLANs, or to provide IP host connectivity to the switch. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly configured. You can configure routing across SVIs.

SVIs are created the first time that you enter the **vlan** interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address.

SVIs support routing protocol and bridging configurations. For more information about configuring IP routing across SVIs, see the "Enabling and Verifying IP Multicast Layer 3 Switching" section on page 164.

Routed Ports

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support subinterfaces. Routed ports can be configured with a Layer 3 routing protocol.

Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the **ip routing** and **router** *protocol* global configuration commands.

⚠ **Caution** Entering a **no switchport** interface configuration command shuts the interface down and then reenables it, which might generate messages on the device to which the interface is connected. Furthermore, when you use this command to put the interface into Layer 3 mode, you are deleting any Layer 2 characteristics configured on the interface. (Also, when you return the interface to Layer 2 mode, you are deleting any Layer 3 characteristics configured on the interface.)

The number of routed ports and SVIs that you can configure is not limited by software; however, the interrelationship between this number and the number of other features being configured might have an impact on CPU utilization because of hardware limitations.

Routed ports support only Cisco Express Forwarding (CEF) switching (IP fast switching is not supported).

IP Multicast Layer 3 Switching

The maximum number of configured VLANs must be less than or equal to 242. The maximum number of multicast groups is related to the maximum number of VLANs. The number of VLANs is determined by multiplying the number of VLANs by the number of multicast groups. For example, the maximum number for 10 VLANs and 20 groups would be 200, under the 242 limit. This feature also provides support for Protocol Independent Multicast (PIM) sparse mode/dense mode/sparse-dense mode.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping constrains the flooding of multicast traffic by dynamically configuring the interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast devices. The LAN switch snoops on the IGMP traffic between the host and the router and keeps track of multicast groups and member ports. When the switch receives an IGMP join report from a host for a particular multicast group, the switch adds the host port number to the associated multicast forwarding table entry. When it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. After it relays the IGMP queries from the multicast router, it deletes entries periodically if it does not receive any IGMP membership reports from the multicast clients.

When IGMP snooping is enabled, the multicast router sends out periodic IGMP general queries to all VLANs. The switch responds to the router queries with only one join request per MAC multicast group, and the switch creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an IGMP join request. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping vlan static** command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

EtherSwitch network modules support a maximum of 255 IP multicast groups and support both IGMP version 1 and IGMP version 2.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

In the IP multicast-source-only environment, the switch learns the IP multicast group from the IP multicast data stream and only forwards traffic to the multicast router ports.

Immediate-Leave Processing

IGMP snooping Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate-Leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

Note You should use the Immediate-Leave processing feature only on VLANs where only one host is connected to each port. If Immediate-Leave processing is enabled on VLANs where more than one host is connected to a port, some hosts might be inadvertently dropped. Immediate-Leave processing is supported only with IGMP version 2 hosts.

Setting the Snooping Method

Multicast-capable router ports are added to the forwarding table for every IP multicast entry. The switch learns of such ports through one of these methods:

- Snooping on PIM and DVMRP packets
- Statically connecting to a multicast router port with the **ip igmp snooping mrouter** global configuration command

You can configure the switch to snoop on PIM/Distance Vector Multicast Routing Protocol (PIM/DVMRP) packets. By default, the switch snoops on PIM/DVMRP packets on all VLANs. To learn of multicast router ports through PIM-DVMRP packets, use the **ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp** interface configuration command.

Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group, it sends an IGMP join message, specifying the IP multicast group it wants to join. When the switch receives this message, it adds the port to the IP multicast group port address entry in the forwarding table.

Refer to Figure 17. Host 1 wants to join multicast group 224.1.2.3 and send a multicast message of an unsolicited IGMP membership report (IGMP join message) to the group with the equivalent MAC destination address of 0100.5E01.0203. The switch recognizes IGMP packets and forwards them to the CPU. When the CPU receives the IGMP multicast report by Host 1, the CPU uses the information to set up a multicast forwarding table entry as shown in Table 9 that includes the port numbers of Host 1 and the router.

Figure 17 Initial IGMP Join Message

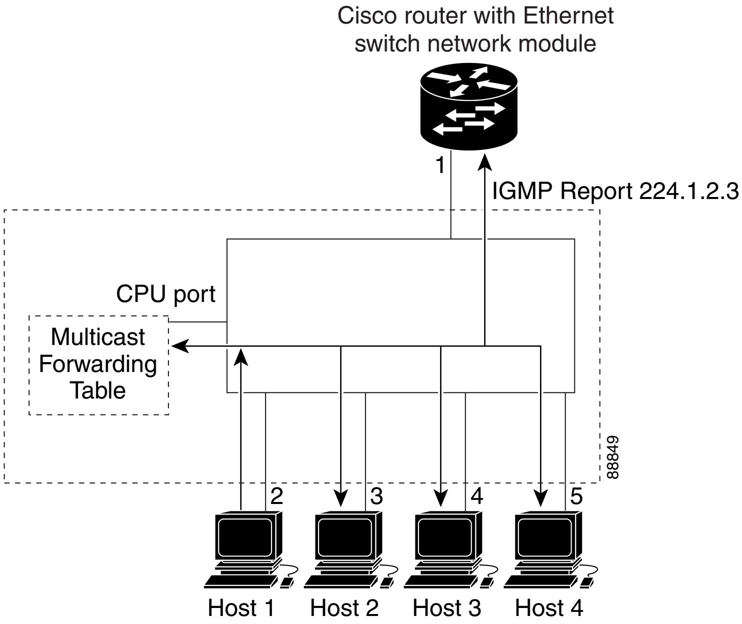

Cisco router with Ethernet switch network module
1
IGMP Report 224.1.2.3
CPU port
Multicast Forwarding Table
2
3
4
5
Host 1
Host 2
Host 3
Host 4
88849

Table 9 IP Multicast Forwarding Table

Destination Address	Type of Packet	Ports
0100.5e01.0203	!IGMP	1, 2

Note that the switch architecture allows the CPU to distinguish IGMP information packets from other packets for the multicast group. The switch recognizes the IGMP packets through its filter engine. This prevents the CPU from becoming overloaded with multicast frames.

The entry in the multicast forwarding table tells the switching engine to send frames addressed to the 0100.5E01.0203 multicast MAC address that are not IGMP packets (!IGMP) to the router and to the host that has joined the group.

If another host (for example, Host 4) sends an IGMP join message for the same group (Figure 18), the CPU receives that message and adds the port number of Host 4 to the multicast forwarding table as shown in Table 10.

Figure 18 Second Host Joining a Multicast Group

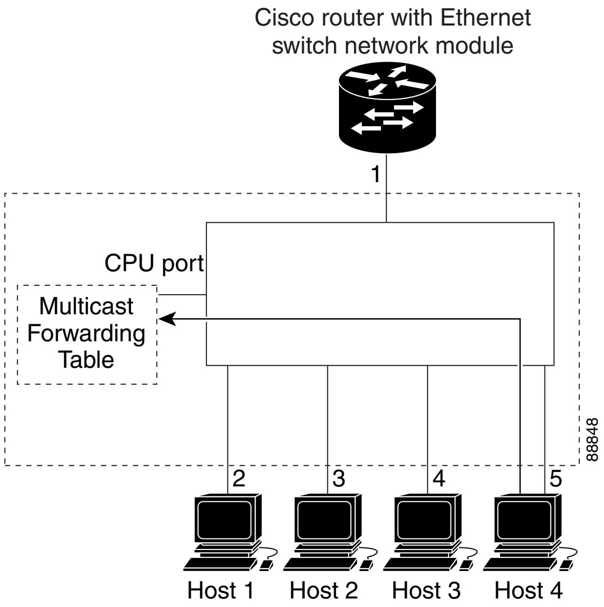

Cisco router with Ethernet switch network module
1
CPU port
Multicast Forwarding Table
2
3
4
5
88848
Host 1
Host 2
Host 3
Host 4

Table 10 Updated Multicast Forwarding Table

Destination Address	Type of Packet	Ports
0100.5e01.0203	!IGMP	1, 2, 5

Leaving a Multicast Group

The router sends periodic IP multicast general queries, and the switch responds to these queries with one join response per MAC multicast group. As long as at least one host in the VLAN needs multicast traffic, the switch responds to the router queries, and the router continues forwarding the multicast traffic to the VLAN. The switch only forwards IP multicast group traffic to those hosts listed in the forwarding table for that IP multicast group.

When hosts need to leave a multicast group, they can either ignore the periodic general-query requests sent by the router, or they can send a leave message. When the switch receives a leave message from a host, it sends out a group-specific query to determine if any devices behind that interface are interested in traffic for the specific multicast group. If, after a number of queries, the router processor receives no reports from a VLAN, it removes the group for the VLAN from its multicast forwarding table.

Fallback Bridging

With fallback bridging, the switch bridges together two or more VLANs or routed ports, essentially connecting multiple VLANs within one bridge domain. Fallback bridging forwards traffic that the multilayer switch does not route and forwards traffic belonging to a nonroutable protocol such as DECnet.

Fallback bridging does not allow the spanning trees from the VLANs being bridged to collapse; each VLAN has its own Spanning Tree Protocol (STP) instance and a separate spanning tree, called the VLAN-bridge spanning tree, which runs on top of the bridge group to prevent loops.

A VLAN bridge domain is represented using the switch virtual interface (SVI). A set of SVIs and routed ports (which do not have any VLANs associated with them) can be configured to form a bridge group.

Recall that an SVI represents a VLAN of switch ports as one interface to the routing or bridging function in the system. Only one SVI can be associated with a VLAN, and it is only necessary to configure an SVI for a VLAN when you want to route between VLANs, to fallback-bridge nonroutable protocols between VLANs, or to provide IP host connectivity to the switch. A routed port is a physical port that acts like a port on a router, but it is not connected to a router. A routed port is not associated with a particular VLAN, does not support subinterfaces, but behaves like a normal routed interface.

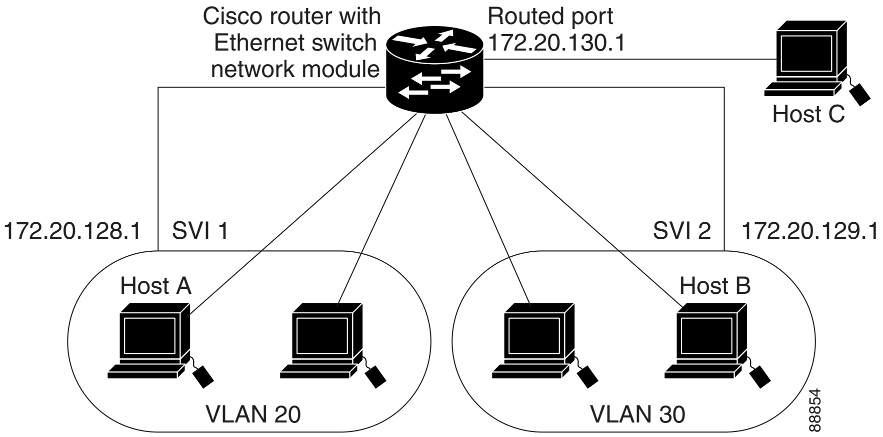
A bridge group is an internal organization of network interfaces on a switch. Bridge groups cannot be used to identify traffic switched within the bridge group outside the switch on which they are defined. Bridge groups on the same switch function as distinct bridges; that is, bridged traffic and bridge protocol data units (BPDUs) cannot be exchanged between different bridge groups on a switch. An interface can be a member of only one bridge group. Use a bridge group for each separately bridged (topologically distinct) network connected to the switch.

The purpose of placing network interfaces into a bridge group is twofold:

- To bridge all nonrouted traffic among the network interfaces making up the bridge group. If the packet destination address is in the bridge table, it is forwarded on a single interface in the bridge group. If the packet destination address is not in the bridge table, it is flooded on all forwarding interfaces in the bridge group. The bridge places source addresses in the bridge table as it learns them during the bridging process.
- To participate in the spanning-tree algorithm by receiving, and in some cases sending, BPDUs on the LANs to which they are attached. A separate spanning process runs for each configured bridge group. Each bridge group participates in a separate spanning-tree instance. A bridge group establishes a spanning-tree instance based on the BPDUs it receives on only its member interfaces.

Figure 19 shows a fallback bridging network example. The multilayer switch has two interfaces configured as SVIs with different assigned IP addresses and attached to two different VLANs. Another interface is configured as a routed port with its own IP address. If all three of these ports are assigned to the same bridge group, non-IP protocol frames can be forwarded among the end stations connected to the switch.

Figure 19 *Fallback Bridging Network Example*



Network Security with ACLs at Layer 2

Network security on your EtherSwitch network module can be implemented using access control lists (ACLs), which are also referred to in commands and tables as access lists.

Understanding ACLs

Packet filtering can limit network traffic and restrict network use by certain users or devices. ACLs can filter traffic as it passes through a switch and permit or deny packets from crossing specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. The switch tests the packet against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing conditions after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet.

You configure access lists on a Layer 2 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at switch interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic.

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions the packet must satisfy in order to match the ACE. The meaning of *permit* or *deny* depends on the context in which the ACL is used.

The EtherSwitch network module supports IP ACLs to filter IP traffic, including TCP or User Datagram Protocol (UDP) traffic (but not both traffic types in the same ACL).

ACLs

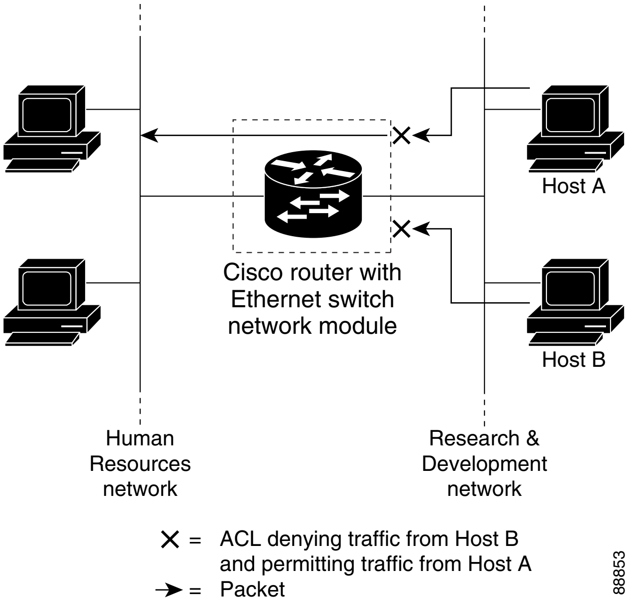
You can apply ACLs on physical Layer 2 interfaces. ACLs are applied on interfaces only on the inbound direction.

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

The switch examines access lists associated with features configured on a given interface and a direction. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL. For example, you can use ACLs to allow one host to access a part of a network, but to prevent another host from accessing the same part. In Figure 20, ACLs applied at the switch input allow Host A to access the Human Resources network, but prevent Host B from accessing the same network.

Figure 20 Using ACLs to Control Traffic to a Network



Handling Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some ACEs do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.
- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Router(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Router(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Router(config)# access-list 102 deny tcp any any
```

Note In the first and second ACEs in the examples, the **eq** keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

- Packet A is a TCP packet from host 10.2.2.2, port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit), as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information because the first ACE only checks Layer 3 information when applied to fragments. (The information in this example is that the packet is TCP and that the destination is 10.1.1.1.)

- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information.
- Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.
- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port FTP. If this packet is fragmented, the first fragment matches the third ACE (a deny). All other fragments also match the third ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

Understanding Access Control Parameters

Before configuring ACLs on the EtherSwitch network module, you must have a thorough understanding of the Access Control Parameters (ACPs). ACPs are referred to as masks in the switch CLI commands, and output.

Each ACE has a mask and a rule. The Classification Field or mask is the field of interest on which you want to perform an action. The specific values associated with a given mask are called *rules*.

Packets can be classified on these Layer 3 and Layer 4 fields.

- Layer 3 fields:
  - IP source address (Specify all 32 IP source address bits to define the flow, or specify a user-defined subnet. There are no restrictions on the IP subnet to be specified.)
  - IP destination address (Specify all 32 IP destination address bits to define the flow, or specify a user-defined subnet. There are no restrictions on the IP subnet to be specified.)

    You can use any combination or all of these fields simultaneously to define a flow.
- Layer 4 fields:
  - TCP (You can specify a TCP source, destination port number, or both at the same time.)
  - UDP (You can specify a UDP source, destination port number, or both at the same time.)

Note A mask can be a combination of multiple Layer 3 and Layer 4 fields.

There are two types of masks:

- User-defined mask—masks that are defined by the user.
- System-defined mask—these masks can be configured on any interface:

```
Router(config-ext-nacl)# permit tcp any any
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# permit udp any any
Router(config-ext-nacl)# deny udp any any
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# deny any any
Router(config-ext-nacl)# permit any any
```

Note In an IP extended ACL (both named and numbered), a Layer 4 system-defined mask cannot precede a Layer 3 user-defined mask. For example, a Layer 4 system-defined mask such as **permit tcp any any** or **deny udp any any** cannot precede a Layer 3 user-defined mask such as **permit ip 10.1.1.1 any**. If you configure this combination, the ACL is not configured. All other combinations of system-defined and user-defined masks are allowed in security ACLs.

The EtherSwitch network module ACL configuration is consistent with Cisco Catalyst switches. However, there are significant restrictions as well as differences for ACL configurations on the EtherSwitch network module.

Guidelines for Configuring ACLs on the EtherSwitch network module

These configuration guidelines apply to ACL filters:

- Only one ACL can be attached to an interface.
- All ACEs in an ACL must have the same user-defined mask. However, ACEs can have different rules that use the same mask. On a given interface, only one type of user-defined mask is allowed, but you can apply any number of system-defined masks.

  The following example shows the same mask in an ACL:

  ```
  Router(config)# ip access-list extended acl2
  Router(config-ext-nacl)# permit tcp 10.1.1.1 0.0.0.0 any eq 80
  Router(config-ext-nacl)# permit tcp 20.1.1.1 0.0.0.0 any eq 23
  ```

  In this example, the first ACE permits all the TCP packets coming from the host 10.1.1.1 with a destination TCP port number of 80. The second ACE permits all TCP packets coming from the host 20.1.1.1 with a destination TCP port number of 23. Both the ACEs use the same mask; therefore, a EtherSwitch network module supports this ACL.
- Only four user-defined masks can be defined for the entire system. These can be used for either security or quality of service (QoS) but cannot be shared by QoS and security. You can configure as many ACLs as you require. However, a system error message appears if ACLs with more than four different masks are applied to interfaces.

Table 11 lists a summary of the ACL restrictions on EtherSwitch network modules.

Table 11 Summary of ACL Restrictions

Restriction	Number Permitted
Number of user-defined masks allowed in an ACL	1
Number of ACLs allowed on an interface	1
Total number of user-defined masks for security and QoS allowed on a switch	4

Quality of Service for the EtherSwitch Network Module

Quality of service (QoS) can be implemented on your EtherSwitch network module. With this feature, you can provide preferential treatment to certain types of traffic. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. It transmits the packets without any assurance of reliability, delay bounds, or throughput.

Understanding Quality of Service)

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

With the QoS feature configured on your EtherSwitch network module, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation for this release is based on the DiffServ architecture, an emerging standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network. The classification is carried in the IP packet header, using six bits from the deprecated IP type of service (ToS) field to carry the classification (*class*) information. Classification can also be carried in the Layer 2 frame. These special bits in the Layer 2 frame or a Layer 3 packet are described here and shown in Figure 21:

- Prioritization values in Layer 2 frames:

  Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On interfaces configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

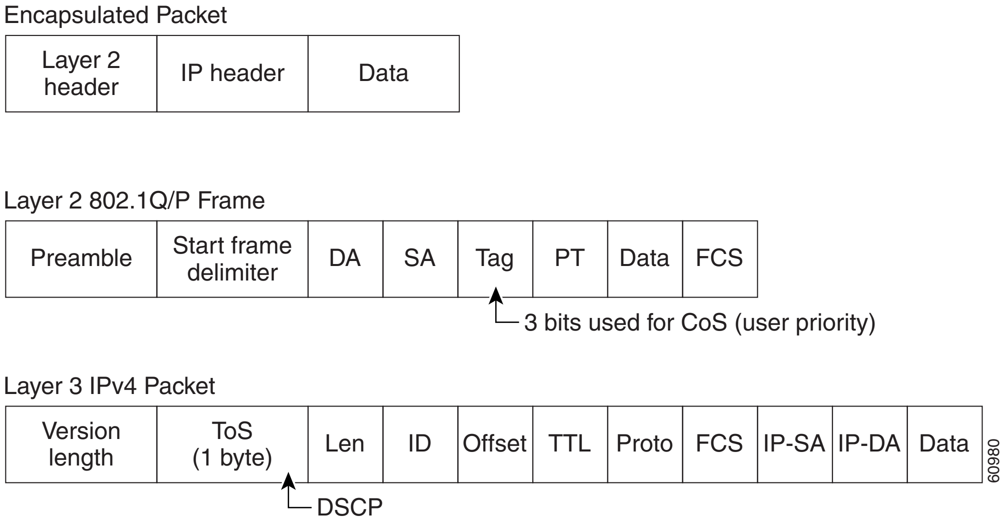
  Other frame types cannot carry Layer 2 CoS values.

  Layer 2 CoS values range from 0 for low priority to 7 for high priority.

- Prioritization bits in Layer 3 packets:

  Layer 3 IP packets can carry a Differentiated Services Code Point (DSCP) value. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

Figure 21 QoS Classification Layers in Frames and Packets



Note Layer 2 ISL Frame is not supported in this release.

Note Layer 3 IPv6 packets are dropped when received by the switch.

All switches and routers across the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to happen closer to the edge of the network so that the core switches and routers are not overloaded.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the DiffServ architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control you need over incoming and outgoing traffic.

The EtherSwitch network module can function as a Layer 2 switch connected to a Layer 3 router. When a packet enters the Layer 2 engine directly from a switch port, it is placed into one of four queues in the dynamic, 32-MB shared memory buffer. The queue assignment is based on the dot1p value in the packet. Any voice bearer packets that come in from the Cisco IP phones on the voice VLAN are automatically placed in the highest priority (Queue 3) based on the 802.1p value generated by the IP phone. The queues are then serviced on a weighted round robin (WRR) basis. The control traffic, which uses a CoS or ToS of 3, is placed in Queue 2.

Table 12 summarizes the queues, CoS values, and weights for Layer 2 QoS on the EtherSwitch network module.

Table 12 Queues, CoS values, and Weights for Layer 2 QoS

Queue Number	CoS Value	Weight
3	5,6,7	255
2	3,4	64
1	2	16
0	0,1	1

The weights specify the number of packets that are serviced in the queue before moving on to the next queue. Voice Realtime Transport Protocol (RTP) bearer traffic marked with a CoS or ToS of 5 and Voice Control plane traffic marked with a CoS/ToS of 3 are placed into the highest priority queues. If the queue has no packets to be serviced, it is skipped. Weighted Random Early Detection (WRED) is not supported on the Fast Ethernet ports.

You cannot configure port-based QoS on the Layer 2 switch ports.

Basic QoS Model

Figure 22 shows the basic QoS model. Actions at the ingress interface include classifying traffic, policing, and marking:

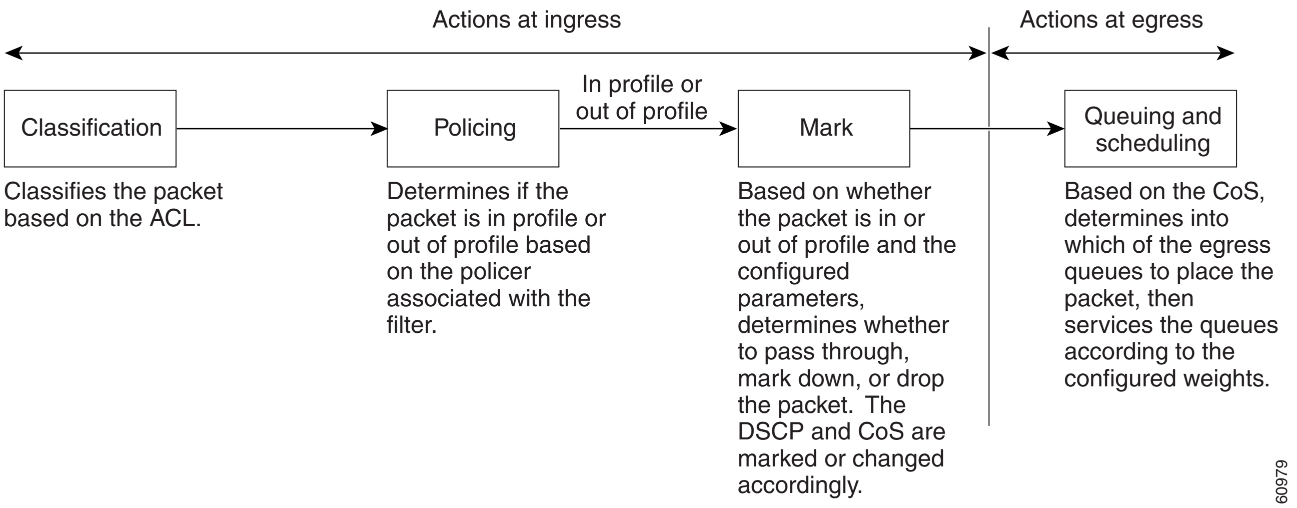
- Classifying distinguishes one kind of traffic from another. For more information, see the "Classification" section on page 112.

- Policing determines whether a packet is in or out of profile according to the configured policer, and the policer limits the bandwidth consumed by a flow of traffic. The result of this determination is passed to the marker. For more information, see the "Policing and Marking" section on page 113.
- Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and decides what to do with the packet (pass through a packet without modification, mark down the DSCP value in the packet, or drop the packet). For more information, see the "Policing and Marking" section on page 113.

Actions at the egress interface include queueing and scheduling:

- Queuing evaluates the CoS value and determines which of the four egress queues in which to place the packet.
- Scheduling services the four egress queues based on their configured WRR weights.

Figure 22 Basic QoS Model


Actions at ingress
Actions at egress
Classification
Policing
In profile or out of profile
Mark
Queuing and scheduling
Classifies the packet based on the ACL.
Determines if the packet is in profile or out of profile based on the policer associated with the filter.
Based on whether the packet is in or out of profile and the configured parameters, determines whether to pass through, mark down, or drop the packet. The DSCP and CoS are marked or changed accordingly.
Based on the CoS, determines into which of the egress queues to place the packet, then services the queues according to the configured weights.
60979

Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet.

Classification occurs only on a physical interface basis. No support exists for classifying packets at the VLAN or the switched virtual interface level.

You specify which fields in the frame or packet that you want to use to classify incoming traffic.

Classification Based on QoS ACLs

You can use IP standard or IP extended ACLs to define a group of packets with the same characteristics (*class*). In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings than with security ACLs:

- If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.
- If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet.
- If multiple ACLs are configured on an interface, the packet matches the first ACL with a permit action, and QoS processing begins.

- Configuration of a deny action is not supported in QoS ACLs on the 16- and 36-port EtherSwitch network modules.
- System-defined masks are allowed in class maps with these restrictions:
  - A combination of system-defined and user-defined masks cannot be used in the multiple class maps that are a part of a policy map.
  - System-defined masks that are a part of a policy map must all use the same type of system mask. For example, a policy map cannot have a class map that uses the **permit tcp any any** ACE and another that uses the **permit ip any any** ACE.
  - A policy map can contain multiple class maps that all use the same user-defined mask or the same system-defined mask.

Note For more information on the system-defined mask, see the "Understanding Access Control Parameters" section on page 108.

- For more information on ACL restrictions, see the "Guidelines for Configuring ACLs on the EtherSwitch network module" section on page 109.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the **access-list** global configuration command.

Classification Based on Class Maps and Policy Maps

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it; the criteria can include matching the access group defined by the ACL. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you further classify it through the use of a policy map.

A policy map specifies which traffic class to act on. Actions can include setting a specific DSCP value in the traffic class or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile. Before a policy map can be effective, you must attach it to an interface.

The policy map can also contain commands that define the policer, the bandwidth limitations of the traffic, and the action to take if the limits are exceeded. For more information, see the "Policing and Marking" section on page 113.

A policy map also has these characteristics:

- A policy map can contain multiple class statements.
- A separate policy-map class can exist for each type of traffic received through an interface.
- A policy-map configuration state supersedes any actions due to an interface trust state.

For configuration information, see the "Configuring a QoS Policy" section on page 191.

Policing and Marking

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer specifies the action to take for packets that are in or out of profile. These actions, carried out by the marker, include dropping the packet, or marking down the packet with a new value that is user-defined.

You can create this type of policer:

Individual—QoS applies the bandwidth limits specified in the policer separately to each matched traffic class. You configure this type of policer within a policy map by using the policy-map configuration command.

For non-IP traffic, you have these marking options:

- Use the port default. If the frame does not contain a CoS value, assign the default port CoS value to the incoming frame.
- Trust the CoS value in the incoming frame (configure the port to trust CoS). Layer 2 802.1Q frame headers carry the CoS value in the three most-significant bits of the Tag Control Information field. CoS values range from 0 for low priority to 7 for high priority.

  The trust DSCP configuration is meaningless for non-IP traffic. If you configure a port with this option and non-IP traffic is received, the switch assigns the default port CoS value and classifies traffic based on the CoS value.

For IP traffic, you have these classification options:

- Trust the IP DSCP in the incoming packet (configure the port to trust DSCP), and assign the same DSCP to the packet for internal use. The IETF defines the six most-significant bits of the 1-byte type of service (ToS) field as the DSCP. The priority represented by a particular DSCP value is configurable. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.
- Trust the CoS value (if present) in the incoming packet, and generate the DSCP by using the CoS-to-DSCP map.

When configuring policing and policers, keep these items in mind:

- By default, no policers are configured.
- Policers can only be configured on a physical port. There is no support for policing at a VLAN or switched virtual interface (SVI) level.
- Only one policer can be applied to a packet in the input direction.
- Only the average rate and committed burst parameters are configurable.
- Policing occurs on the ingress interfaces:
  - 60 policers are supported on ingress Gigabit-capable Ethernet ports.
  - 6 policers are supported on ingress 10/100 Ethernet ports.
  - Granularity for the average burst rate is 1 Mbps for 10/100 ports and 8 Mbps for Gigabit Ethernet ports.
- On an interface configured for QoS, all traffic received through the interface is classified, policed, and marked according to the policy map attached to the interface. On a trunk interface configured for QoS, traffic in *all* VLANs received through the interface is classified, policed, and marked according to the policy map attached to the interface.
- VLAN-based egress DSCP-to-COS mapping is supported. DSCP-to-COS mapping occurs for all packets with a specific VLAN ID egressing from the CPU to the physical port. The packets can be placed in the physical port egress queue depending on the COS value. Packets are handled according to type of service.

Note No policers can be configured on the egress interface on EtherSwitch network modules.

Mapping Tables

The EtherSwitch network modules support these types of marking to apply to the switch:

- CoS value to the DSCP value
- DSCP value to CoS value

Note An interface can be configured to trust either CoS or DSCP, but not both at the same time.

Before the traffic reaches the scheduling stage, QoS uses the configurable DSCP-to-CoS map to derive a CoS value from the internal DSCP value.

The CoS-to-DSCP and DSCP-to-CoS map have default values that might or might not be appropriate for your network.

How to Configure the EtherSwitch Network Module

This section contains the following tasks:

- Configuring VLANs, page 116 (required)
- Configuring VLAN Trunking Protocol, page 118 (optional)
- Configuring Spanning Tree on a VLAN, page 120 (required)
- Verifying Spanning Tree on a VLAN, page 123 (optional)
- Configuring Layer 2 Interfaces, page 125 (required)
- Configuring an Ethernet Interface as a Layer 2 Trunk, page 128 (optional)
- Configuring an Ethernet Interface as a Layer 2 Access, page 130 (optional)
- Configuring Separate Voice and Data VLANs, page 131 (optional)
- Configuring a Single Voice and Data VLAN, page 133 (optional)
- Managing the EtherSwitch network module, page 134 (required)
- Configuring Voice Ports, page 137 (required)
- Verifying Cisco Discovery Protocol, page 139 (optional)
- Configuring the MAC Table to Provide Port Security, page 140 (required)
- Configuring 802.1x Authentication, page 143 (optional)
- Configuring Power Management on the Interfaces, page 152 (optional)
- Configuring Storm Control, page 153 (optional)
- Configuring Layer 2 EtherChannels (Port-Channel Logical Interfaces), page 156 (required)
- Configuring Flow Control on Gigabit Ethernet Ports, page 159 (required)
- Configuring Intrachassis Stacking, page 160 (required)
- Configuring Switched Port Analyzer (SPAN), page 161 (required)
- Configuring Layer 3 Interfaces, page 162 (required)
- Enabling and Verifying IP Multicast Layer 3 Switching, page 164 (required)
- Configuring IGMP Snooping, page 166 (optional)
- Configuring Fallback Bridging, page 168 (optional)

- Configuring Network Security with ACLs at Layer 2, page 175 (optional)
- Configuring Quality of Service (QoS) on the EtherSwitch network module, page 187 (optional)
- Configuring a QoS Policy, page 191 (optional)

Configuring VLANs

Perform this task to configure the VLANs on an EtherSwitch network module.

VLAN Removal from the Database

When you delete a VLAN from a router with an EtherSwitch network module installed that is in VTP server mode, the VLAN is removed from all EtherSwitch routers and switches in the VTP domain. When you delete a VLAN from an EtherSwitch router or switch that is in VTP transparent mode, the VLAN is deleted only on that specific device.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vlan** *vlan-id* [**are** *hops*] [**backupcrf** *mode*] [**bridge** *type* | *number*] [**media** *type*] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *sa-id-value*] [**state** {**suspend** | **active**}] [**stp type** *type*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
4. **no vlan** *vlan-id*
5. **exit**
6. **show vlan-switch** [**brief** | **id** *vlan* | **name** *name*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`vlan database`**
	Example:
	`Router# configure terminal`
		Enters VLAN configuration mode.

	Command or Action	Purpose

Step 3	**`vlan`** *`vlan-id`* `[`**`are`** *`hops`*`] [`**`backupcrf`** *`mode`*`] [`**`bridge`** *`type`* `|` *`number`*`] [`**`media`** *`type`*`] [`**`mtu`** *`mtu-size`*`] [`**`name`** *`vlan-name`*`] [`**`parent`** *`parent-vlan-id`*`] [`**`ring`** *`ring-number`*`] [`**`said`** *`sa-id-value`*`] [`**`state`** `{`**`suspend`** `|` **`active`**`}] [`**`stp type`** *`type`*`] [`**`tb-vlan1`** *`tb-vlan1-id`*`] [`**`tb-vlan2`** *`tb-vlan2-id`*`]`
	Example:
	`Router(vlan)# vlan 2 media ethernet name vlan1502`
		Configures a specific VLAN.
		• In this example, Ethernet VLAN 2 is added with the name of vlan1502.
		• The VLAN database is updated when you leave VLAN configuration mode.

Step 4	**`no vlan`** *`vlan-id`*
	Example:
	`Router(vlan)# no vlan 2`
		(Optional) Deletes a specific VLAN.
		• In this example, VLAN 2 is deleted.

Step 5	**`exit`**
	Example:
	`Router(vlan)# exit`
		Exits VLAN configuration mode and returns the router to privileged EXEC mode.

Step 6	**`show vlan-switch`** `[`**`brief`** `|` **`id`** *`vlan`* `|` **`name`** *`name`*`]`
	Example:
	`Router# show vlan-switch name vlan0003`
		(Optional) Displays VLAN information.
		• The optional **brief** keyword displays only a single line for each VLAN, naming the VLAN, status, and ports.
		• The optional **id** keyword displays information about a single VLAN identified by VLAN ID number; valid values are from 1 to 1005.
		• The optional **name** keyword displays information about a single VLAN identified by VLAN name; valid values are an ASCII string from 1 to 32 characters.

Examples

Sample Output for the show vlan-switch Command

In the following example, output information is displayed to verify the VLAN configuration:

```
Router# show vlan-switch name vlan0003

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
```

```
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

In the following example, the **brief** keyword is used to verify that VLAN 2 has been deleted:

```
Router# show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/9, Fa0/14, Gi0/0
3    VLAN0003                         active    Fa0/4, Fa0/5, Fa0/10, Fa0/11
4    VLAN0004                         active    Fa0/6, Fa0/7, Fa0/12, Fa0/13
5    VLAN0005                         active
40   VLAN0040                         active    Fa0/15
50   VLAN0050                         active
1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Configuring VLAN Trunking Protocol

Perform this task to configure the VLAN Trunking Protocol (VTP) on an EtherSwitch network module.

VTP Mode Behavior

When a router with an EtherSwitch network module installed is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network.

When the router is in VTP client mode, you cannot change the VLAN configuration on the device. The client device receives VTP updates from a VTP server in the management domain and modifies its configuration accordingly.

When you configure the router as VTP transparent, you disable VTP on the device. A VTP transparent device does not send VTP updates and does not act on VTP updates received from other devices. However, a VTP transparent device running VTP version 2 does forward received VTP advertisements out all of its trunk links.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vtp server**
4. **vtp domain** *domain-name*
5. **vtp password** *password-value*
6. **vtp client**
7. **vtp transparent**
8. **vtp v2-mode**
9. **exit**
10. **show vtp** {**counters** | **status**}

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`vlan database`**
	Example:
	`Router# vlan database`
		Enters VLAN configuration mode.

Step 3	**`vlan server`**
	Example:
	`Router(vlan)# vlan server`
		Configures the EtherSwitch network module as a VTP server.

Step 4	**`vtp domain`** *`domain-name`*
	Example:
	`Router(vlan)# vtp domain Lab_Network`
		Defines the VTP domain name.
		• The *domain-name* argument consists of up to 32 characters.

Step 5	**`vtp password`** *`password-value`*
	Example:
	`Router(vlan)# vtp password labpassword`
		(Optional) Sets a password for the VTP domain.
		• The *password-value* argument can consist of 8 to 64 characters.

Step 6	**`vtp client`**
	Example:
	`Router(vlan)# vtp client`
		(Optional) Configures the EtherSwitch network module as a VTP client.
		• The VLAN database is updated when you leave VLAN configuration mode.
		Note You would configure the device as either a VTP server or a VTP client.

Step 7	**`vtp transparent`**
	Example:
	`Router(vlan)# vtp transparent`
		(Optional) Disables VTP on the EtherSwitch network module.

Step 8	**`vtp v2-mode`**
	Example:
	`Router(vlan)# vtp v2-mode`
		(Optional) Enables VTP version 2.

	Command or Action	Purpose

Step 9	`exit`
	Example:
	`Router(vlan)# exit`
		Exits VLAN configuration mode and returns the router to global configuration mode.

Step 10	**`show vtp`** `{`**`counters`** `|` **`status`**`}`
	Example:
	`Router# show vtp status`
		(Optional) Displays VTP information.
		• The optional **counters** keyword displays the VTP counters for the EtherSwitch network module.
		• The optional **status** keyword displays general information about the VTP management domain.

Examples

Sample Output for the show vtp Command

In the following example, output information about the VTP management domain is displayed:

```
Router# show vtp status

VTP Version                     : 2
Configuration Revision          : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 33
VTP Operating Mode              : Client
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
```

Configuring Spanning Tree on a VLAN

Perform this task to enable spanning tree on a per-VLAN basis and configure various spanning tree features. The EtherSwitch network module maintains a separate instance of spanning tree for each VLAN (except on VLANs on which you disable spanning tree).

VLAN Root Bridge

The EtherSwitch network module maintains a separate instance of spanning tree for each active VLAN configured on the device. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID will become the root bridge for that VLAN.

To configure a VLAN instance to become the root bridge, the bridge priority can be modified from the default value (32768) to a significantly lower value so that the bridge becomes the root bridge for the specified VLAN. Use the **spanning-tree vlan** *vlan-id* **root** command to alter the bridge priority.

The switch checks the bridge priority of the current root bridges for each VLAN. The bridge priority for the specified VLANs is set to 8192 if this value will cause the switch to become the root for the specified VLANs.

If any root switch for the specified VLANs has a bridge priority lower than 8192, the switch sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

For example, if all switches in the network have the bridge priority for VLAN 100 set to the default value of 32768, entering the **spanning-tree vlan 100 root primary** command on a switch will set the bridge priority for VLAN 100 to 8192, causing the switch to become the root bridge for VLAN 100.

Note The root bridge for each instance of spanning tree should be a backbone or distribution switch device. Do not configure an access switch device as the spanning tree primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically picks an optimal hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the spanning tree convergence time. You can use the **hello-time** keyword to override the automatically calculated hello time.

Note You should avoid configuring the hello time, forward delay time, and maximum age time manually after configuring the switch as the root bridge.

VLAN Bridge Priority

Caution Exercise care when using the **spanning-tree vlan** command with the **priority** keyword. For most situations **spanning-tree vlan** with the **root primary** keywords and the **spanning-tree vlan** with the **root secondary** keywords are the preferred commands to modify the bridge priority.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **spanning-tree vlan** *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **protocol** *protocol* | [**root** {**primary** | **secondary**} [**diameter** *net-diameter*] [**hello-time** *seconds*]]]]
4. **spanning-tree vlan** *vlan-id* [**priority** *priority*]
5. **spanning-tree vlan** *vlan-id* [**root** {**primary** | **secondary**} [**diameter** *net-diameter*] [**hello-time** *seconds*]]
6. **spanning-tree vlan** *vlan-id* [**hello-time** *seconds*]
7. **spanning-tree vlan** *vlan-id* [**forward-time** *seconds*]
8. **spanning-tree vlan** *vlan-id* [**max-age** *seconds*]
9. **spanning-tree backbonefast**
10. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
11. **spanning-tree port-priority** *port-priority*
12. **spanning-tree cost** *cost*
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**spanning-tree vlan** *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **protocol** *protocol* | [**root** {**primary** | **secondary**} [**diameter** *net-diameter*] [**hello-time** *seconds*]]]] **Example:** `Router(config)# spanning-tree vlan 200`	Configures spanning tree on a per-VLAN basis. • In this example, spanning tree is enabled on VLAN 200. • Use the **no** form of this command to disable spanning tree on the specified VLAN.
Step 4	**spanning-tree vlan** *vlan-id* [**priority** *priority*] **Example:** `Router(config)# spanning-tree vlan 200 priority 33792`	(Optional) Configures the bridge priority of a VLAN. • The *priority* value can be from 1 to 65535. • Review the "VLAN Bridge Priority" section before using this command. • Use the **no** form of this command to restore the defaults.
Step 5	**spanning-tree vlan** *vlan-id* [**root** {**primary** | **secondary**} [**diameter** *net-diameter*] [**hello-time** *seconds*]] **Example:** `Router(config)# spanning-tree vlan 200 root primary diameter 4`	(Optional) Configures the EtherSwitch network module as the root bridge. • Review the "VLAN Root Bridge" concept before using this command.
Step 6	**spanning-tree vlan** *vlan-id* [**hello-time** *seconds*] **Example:** `Router(config)# spanning-tree vlan 200 hello-time 7`	(Optional) Configures the hello time of a VLAN. • The *seconds* value can be from 1 to 10 seconds. • In this example, the hello time is set to 7 seconds.
Step 7	**spanning-tree vlan** *vlan-id* [**forward-time** *seconds*] **Example:** `Router(config)# spanning-tree vlan 200 forward-time 21`	(Optional) Configures the spanning tree forward delay time of a VLAN. • The *seconds* value can be from 4 to 30 seconds. • In this example, the forward delay time is set to 21 seconds.

	Command or Action	Purpose
Step 8	**spanning-tree vlan** *vlan-id* [**max-age** *seconds*] **Example:** `Router(config)# spanning-tree vlan 200 max-age 36`	(Optional) Configures the maximum aging time of a VLAN. • The *seconds* value can be from 6 to 40 seconds. • In this example, the maximum number of seconds that the information in a BPDU is valid is set to 36 seconds.
Step 9	**spanning-tree backbonefast** **Example:** `Router(config)# spanning-tree vlan 200 max-age 36`	(Optional) Enables BackboneFast on the EtherSwitch network module. • Use this command to detect indirect link failures and to start the spanning tree reconfiguration sooner. **Note** If you use BackboneFast, you must enable it on all switch devices in the network. BackboneFast is not supported on Token Ring VLANs but it is supported for use with third-party switches.
Step 10	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot***/***port* **Example:** `Router(config)# interface fastethernet 5/8`	Selects the Ethernet interface to configure and enters interface configuration mode. • The *slot***/***port* argument identifies the slot and port numbers of the interface. The space between the interface name and number is optional.
Step 11	**spanning-tree port-priority** *port-priority* **Example:** `Router(config-if)# spanning-tree port-priority 64`	(Optional) Configures the port priority for an interface. • The *port-priority* value can be from 1 to 255 in increments of 4.
Step 12	**spanning-tree cost** *cost* **Example:** `Router(config-if)# spanning-tree cost 18`	(Optional) Configures the port cost for an interface. • The *cost* value can be from 1 to 200000000 (1 to 65535 in Cisco IOS Releases 12.1(2)E and earlier).
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode.

Verifying Spanning Tree on a VLAN

Perform this optional task to verify the spanning tree configuration on a VLAN.

SUMMARY STEPS

1. **enable**
2. **show spanning-tree** [*bridge-group*] [**active** | **backbonefast** | **blockedports** | **bridge** | **brief** | **inconsistentports** | **interface** *interface-type interface-number* | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show spanning-tree** [*bridge-group*] [**active** | **backbonefast** | **blockedports** | **bridge** | **brief** | **inconsistentports** | **interface** *interface-type interface-number* | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*]

Use this command with the **vlan** keyword to display spanning tree information about a specified VLAN:

```
Router# show spanning-tree vlan 200

VLAN200 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0050.3e8d.6401
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 16384, address 0060.704c.7000
  Root port is 264 (FastEthernet5/8), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 01:53:48 ago
  Times:  hold 1, topology change 24, notification 2
          hello 2, max age 14, forward delay 10
  Timers: hello 0, topology change 0, notification 0


 Port 264 (FastEthernet5/8) of VLAN200 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 129.9.
   Designated root has priority 16384, address 0060.704c.7000
   Designated bridge has priority 32768, address 00e0.4fac.b000
   Designated port id is 128.2, designated path cost 19
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 3, received 3417
```

Use this command with the **interface** keyword to display spanning tree information about a specified interface:

```
Router# show spanning-tree interface fastethernet 5/8

Port 264 (FastEthernet5/8) of VLAN200 is forwarding
   Port path cost 19, Port priority 100, Port Identifier 129.8.
   Designated root has priority 32768, address 0010.0d40.34c7
   Designated bridge has priority 32768, address 0010.0d40.34c7
   Designated port id is 128.1, designated path cost 0
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 0, received 13513
```

Use this command with the **bridge**, **brief**, and **vlan** keywords to display the bridge priority information:

```
Router# show spanning-tree bridge brief vlan 200

    Hello Max  Fwd
Vlan                   Bridge ID      Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          33792 0050.3e8d.64c8    2   20    15  ieee
```

Configuring Layer 2 Interfaces

Perform this task to configure a range of interfaces, define a range macro, set the interface speed, set the duplex mode, and add a description for the interface.

Interface Speed and Duplex Mode Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- If both ends of the line support autonegotiation, Cisco highly recommends the default autonegotiation settings.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- Both ends of the line need to be configured to the same setting. For example, both hard-set or both auto-negotiate. Mismatched settings are not supported.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface range** {**vlan** *vlan-id* **-** *vlan-id*} | {{**ethernet** | **fastethernet** | **macro** *macro-name*} *slot***/***interface* **-** *interface*} [**,** {{**ethernet** | **fastethernet** | **macro** *macro-name*} *slot***/***interface* **-** *interface*}]
4. **define interface-range** *macro-name* {**vlan** *vlan-id* **-** *vlan-id*} | {{**ethernet** | **fastethernet**} *slot***/***interface* **-** *interface*} [**,** {{**ethernet** | **fastethernet**} *slot***/***interface* **-** *interface*}]
5. **interface fastethernet** *slot***/***interface*
6. **speed** [**10** | **100** | **auto**]
7. **duplex** [**auto** | **full** | **half**]
8. **description** *string*
9. **exit**
10. **show interfaces fastethernet** *slot***/***port*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**interface range** {**vlan** *vlan-id* **-** *vlan-id*} | {{**ethernet** | **fastethernet** | **macro** *macro-name*} *slot***/***interface* - *interface*}[**,** {{**ethernet** | **fastethernet** | **macro** *macro-name*} *slot***/***interface* **-** *interface*}] **Example:** `Router(config)# interface range fastethernet 5/1 - 4`	Selects the range of interfaces to be configured. - The space before and after the dash is required. For example, the command **interface range fastethernet 1 - 5** is valid; the command **interface range fastethernet 1-5** is not valid. - You can enter one macro or up to five comma-separated ranges. - Comma-separated ranges can include both VLANs and physical interfaces. - You are not required to enter spaces before or after the comma. The **interface range** command only supports VLAN interfaces that are configured with the **interface vlan** command.
Step 4	**define interface-range** *macro-name* {**vlan** *vlan-id* **-** *vlan-id*} | {{**ethernet** | **fastethernet**} *slot***/***interface* **-** *interface*} [**,** {{**ethernet** | **fastethernet**} *slot***/***interface* **-** *interface*}] **Example:** `Router(config)# define interface-range sales vlan 2 - 5`	- Defines the interface range macro and saves it in NVRAM. - In this example, the interface range macro is named sales and contains VLAN numbers from 2 to 5.
Step 5	**interface fastethernet** *slot***/***interface* **Example:** `Router(config)# interface fastethernet 1/4`	Configures a specific Fast Ethernet interface.
Step 6	**speed** [**10** | **100** | **auto**] **Example:** `Router(config-if)# speed 100`	Sets the speed for a Fast Ethernet interface. **Note** If you set the interface speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are autonegotiated.

	Command or Action	Purpose
Step 7	**duplex** [**auto** | **full** | **half**] **Example:** `Router(config-if)# duplex full`	Sets the duplex mode for an Ethernet or Fast Ethernet interface. **Note** If you set the port speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are autonegotiated. You cannot change the duplex mode of autonegotiation interfaces.
Step 8	**description** *string* **Example:** `Router(config-if)# description salesgroup1`	Adds a description for an interface.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. - Repeat this step one more time to exit global configuration mode.
Step 10	**show interfaces fastethernet** *slot***/***port* **Example:** `Router# show interfaces fastethernet 1/4`	(Optional) Displays information about Fast Ethernet interfaces.

Examples

Sample Output for the show interfaces fastethernet Command

In the following example, output information is displayed to verify the speed and duplex mode of a Fast Ethernet interface:

```
Router# show interfaces fastethernet 1/4

FastEthernet1/4 is up, line protocol is down
  Hardware is Fast Ethernet, address is 0000.0000.0c89 (bia 0000.0000.0c89)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  ARP type: ARPA, ARP Timeout 04:00:00
  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 input packets with dribble condition detected
     3 packets output, 1074 bytes, 0 underruns(0/0/0)
     0 output errors, 0 collisions, 5 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Configuring an Ethernet Interface as a Layer 2 Trunk

Perform this task to configure an Ethernet interface as a Layer 2 trunk.

Restrictions

Note Ports do not support Dynamic Trunk Protocol (DTP). Ensure that the neighboring switch is set to a mode that will not send DTP traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **shutdown**
5. **switchport mode** {**access** | **trunk**}
6. **switchport trunk** {**encapsulation dot1q** | **native vlan** | **allowed vlan** *vlan-list*}
7. **switchport trunk allowed vlan** {**add** | **except** | **none** | **remove**} *vlan1*[,*vlan*[,*vlan*[,...]]
8. **no shutdown**
9. **exit**
10. **show interfaces fastethernet** *slot*/*port* {**switchport** | **trunk**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port* **Example:** `Router(config)# interface fastethernet 5/8`	Selects the Ethernet interface to configure.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete. **Note** Encapsulation is always dot1q.

	Command or Action	Purpose

Step 5	**switchport mode** {**access** | **trunk**}
	Example:
	`Router(config-if)# switchport mode trunk`
		Configures the interface type.
		• In this example, the interface type is set to be trunk.

Step 6	**switchport trunk** [**encapsulation dot1q** | **native vlan** | **allowed vlan** *vlan-list*] **Example:** `Router(config-if)# switchport trunk native vlan`	Specifies the trunk options when the interface is in trunking mode. • In this example, native VLAN is set for the trunk in 802.1Q trunking mode.
Step 7	**switchport trunk allowed vlan** {**add** | **except** | **none** | **remove**} *vlan1*[**,***vlan*[**,***vlan*[**,**...]] **Example:** `Router(config-if)# switchport trunk allowed vlan add 2,3,4,5`	(Optional) Configures the list of VLANs allowed on the trunk. • All VLANs are allowed by default. • You cannot remove any of the default VLANs from a trunk.
Step 8	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the interface. (Required only if you shut down the interface.)
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this step one more time to exit global configuration mode.

Step 10	**show interfaces fastethernet** *slot***/***port* {**switchport** | **trunk**}
	Example:
	`Router# show interfaces fastethernet 5/8 switchport`
		(Optional) Displays information about Fast Ethernet interfaces.

Examples

Sample Output for the show interfaces fastethernet Command

In the following two examples, output information is displayed to verify the configuration of Fast Ethernet interface as a Layer 2 trunk:

```
Router# show interfaces fastethernet 5/8 switchport

Name: Fa5/8
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Disabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Protected: false
```

```
Unknown unicast blocked: false
Unknown multicast blocked: false
Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
Voice VLAN: none
Appliance trust: none

Router# show interfaces fastethernet 5/8 trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa1/15    off          802.1q         not-trunking  1
Port      Vlans allowed on trunk
Fa1/15    1
Port      Vlans allowed and active in management domain
Fa1/15    1
Port      Vlans in spanning tree forwarding state and not pruned
Fa1/15    1
```

Configuring an Ethernet Interface as a Layer 2 Access

Perform this task to configure an Ethernet interface as a Layer 2 access.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **shutdown**
5. **switchport mode** {**access** | **trunk**}
6. **switchport access vlan** *vlan-id*
7. **no shutdown**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot***/***port* **Example:** `Router(config)# interface fastethernet 1/0`	Selects the Ethernet interface to configure.
Step 4	**shutdown** **Example:** `Router(config-if)# shutdown`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete. **Note** Encapsulation is always dot1q.

Step 5	**switchport mode** {**access** | **trunk**}
	Example:
	`Router(config-if)# switchport mode access`
		Configures the interface type.
		• In this example, the interface type is set to be Layer 2 access.

Step 6	**switchport access vlan** *vlan* **Example:** `Router(config-if)# switchport access vlan 5`	For access ports, specifies the access VLAN. • In this example, the Layer 2 access VLAN 5 is set.
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the interface. (Required only if you shut down the interface.)
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this step one more time to exit global configuration mode.

Configuring Separate Voice and Data VLANs

Perform this task to configure separate voice and data VLANs on the EtherSwitch network module.

Separate Voice and Data VLANs

For ease of network administration and increased scalability, network managers can configure the EtherSwitch network module to support Cisco IP phones such that the voice and data traffic reside on separate VLANs. We recommend configuring separate VLANs when you are able to segment the existing IP address space of your branch office.

User priority bits in the 802.1p portion of the 802.1Q standard header are used to provide prioritization in Ethernet switches. This is a vital component in designing Cisco AVVID networks.

The EtherSwitch network module provides the performance and intelligent services of Cisco IOS software for branch office applications. The EtherSwitch network module can identify user applications—such as voice or multicast video—and classify traffic with the appropriate priority levels. QoS policies are enforced using Layer 2 and 3 information such as 802.1p, IP precedence, and DSCP.

Note Refer to the *Cisco AVVID QoS Design Guide* for more information on how to implement end-to-end QoS as you deploy Cisco AVVID solutions.

Voice Traffic and Voice VLAN ID (VVID) Using the EtherSwitch Network Module

The EtherSwitch network module can automatically configure voice VLAN. This capability overcomes the management complexity of overlaying a voice topology onto a data network while maintaining the quality of voice traffic. With the automatically configured voice VLAN feature, network administrators can segment phones into separate logical networks, even though the data and voice infrastructure is physically the same. The voice VLAN feature places the phones into their own VLANs without the need for end-user intervention. A user can plug the phone into the switch, and the switch provides the phone with the necessary VLAN information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **switchport mode** {**access** | **trunk**}
5. **switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port* **Example:** `Router(config)# interface fastethernet 5/1`	Selects the Ethernet interface to configure and enters interface configuration mode.

Step 4	**switchport mode** {**access** | **trunk**}
	Example:
	`Router(config-if)# switchport mode trunk`
		Configures the interface type.
		• In this example, the interface type is set to trunk mode.

	Command or Action	Purpose

Step 5	**switchport voice vlan** {*vlan*-id | **dot1p** | **none** | **untagged**}
	Example:
	`Router(config-if)# switchport voice vlan 150`
		Configures the voice port with a VVID that will be used exclusively for voice traffic.
		• In this example, VLAN 150 will be used for voice traffic.

Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this step one more time to exit global configuration mode.

Configuring a Single Voice and Data VLAN

Perform this task to configure a Cisco IP phone to send voice and data traffic on the same VLAN on the EtherSwitch network module.

Single Voice and Data VLAN

For network designs with incremental IP telephony deployment, network managers can configure the EtherSwitch network module so that the voice and data traffic coexist on the same subnet. This might be necessary when it is impractical either to allocate an additional IP subnet for IP phones or to divide the existing IP address space into an additional subnet at the remote branch, it might be necessary to use a single IP address space for branch offices. (This is one of the simpler ways to deploy IP telephony.) When this is the case, you must still prioritize voice above data at both Layer 2 and Layer 3.

Layer 3 classification is already handled because the phone sets the type of service (ToS) bits in all media streams to an IP Precedence value of 5. (With Cisco CallManager Release 3.0(5), this marking changed to a Differentiated Services Code Point ([DSCP]) value of EF.) However, to ensure that there is Layer 2 classification for admission to the multiple queues in the branch office switches, the phone must also use the User Priority bits in the Layer 2 802.1p header to provide class of service (CoS) marking. Setting the bits to provide marking can be done by having the switch look for 802.1p headers on the native VLAN.

This configuration approach must address two key considerations:

- Network managers should ensure that existing subnets have enough available IP addresses for the new Cisco IP phones, each of which requires a unique IP address.
- Administering a network with a mix of IP phones and workstations on the same subnet might pose a challenge.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **switchport access vlan** *vlan-id*
5. **switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface`** {**`ethernet`** | **`fastethernet`** | **`gigabitethernet`**} *`slot`***`/`***`port`*
	Example:
	`Router(config)# interface fastethernet 5/2`
		Selects the Ethernet interface to configure and enters interface configuration mode.

Step 4	**`switchport access vlan`** *`vlan-id`*
	Example:
	`Router(config-if)# switchport access vlan 40`
		Configures the port as an access port and assigns a VLAN.
		• The value of *vlan-id* represents the ID of the VLAN that is sending and receiving untagged traffic on the port. Valid IDs are from 1 to 1001. Leading zeroes are not accepted.

Step 5	**`switchport voice vlan`** {*`vlan`*`-id` | **`dot1p`** | **`none`** | **`untagged`**}
	Example:
	`Router(config-if)# switchport voice vlan dot1p`
		Configures the Cisco IP phone to send voice traffic with higher priority (CoS=5 on 802.1Q tag) on the access VLAN. Data traffic (from an attached PC) is sent untagged for lower priority (port default=0).

Step 6	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode and returns the router to global configuration mode.
		• Repeat this step one more time to exit global configuration mode.

Managing the EtherSwitch network module

Use this task to perform basic management tasks such as adding a trap manager and assigning IP information on the EtherSwitch network module with the Cisco IOS CLI. You might find this information useful when you configure the EtherSwitch network module for the previous scenarios.

Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, community strings for each member switch must be unique. If a member switch has an IP address assigned to it, the management station accesses the switch by using its assigned IP address.

By default, no trap manager is defined, and no traps are issued.

IP Addressing

The recommended configuration for using multiple cables to connect IP phones to the Cisco AVVID network is to use a separate IP subnet and separate VLANs for IP telephony.

IP Information Assigned to the Switch

You can use a BOOTP server to automatically assign IP information to the switch; however, the BOOTP server must be set up in advance with a database of physical MAC addresses and corresponding IP addresses, subnet masks, and default gateway addresses. In addition, the switch must be able to access the BOOTP server through one of its ports. At startup, a switch without an IP address requests the information from the BOOTP server; the requested information is saved in the switch running the configuration file. To ensure that the IP information is saved when the switch is restarted, save the configuration by entering the **write memory** command in privileged EXEC mode.

You can change the information in these fields. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

Use of Ethernet Ports to Support Cisco IP Phones with Multiple Ports

You might want to use multiple ports to connect the Cisco IP phones if any of the following conditions apply to your Cisco IP telephony network:

- You are connecting Cisco IP phones that do not have a second Ethernet port for attaching a PC.
- You want to create a physical separation between the voice and data networks.
- You want to provide in-line power easily to the IP phones without having to upgrade the data infrastructure.

You want to limit the number of switches that need Uninterruptible Power Supply (UPS) power.

Domain Name Mapping and DNS Configuration

Each unique IP address can have a host name associated with it. IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the FTP system, for example, is identified as *ftp.cisco.com*.

To track domain names, IP has defined the concept of a domain name server (DNS), the purpose of which is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet's global naming scheme that uniquely identifies network devices.

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name has that domain name appended to it before being added to the host table.

You can specify up to six hosts that can function as a name server to supply name information for the DNS.

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet's global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

ARP Table Management

To communicate with a device (on Ethernet, for example), the software first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

When you manually add entries to the ARP Table by using the CLI, you must be aware that these entries do not age and must be manually removed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]
4. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
5. **ip address** *ip-address*
6. **exit**
7. **ip default-gateway** *ip-address*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*] Example: `Router(config)# snmp-server host 10.6.1.1 traps 1 snmp vlan-membership`	Enters the trap manager IP address, community string, and the traps to generate.
Step 4	**interface vlan** *vlan-id* Example: `Router(config)# interface vlan 200`	Enters interface configuration mode, and specifies the VLAN to which the IP information is assigned. • VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.
Step 5	**ip address** *ip-address* Example: `Router(config-if)# ip address 10.2.1.2`	Enters the IP address and subnet mask.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode.
Step 7	**ip default-gateway** *ip-address* Example: `Router(config)# ip default-gateway 10.5.1.5`	Enters the IP address of the default routing device.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.

Configuring Voice Ports

Perform this task to instruct the Cisco 7960 IP phone to give voice traffic a higher priority and to forward all traffic through the 802.1Q native VLAN on the EtherSwitch network module. This task also disables inline power to a Cisco 7960 IP phone to allow voice traffic to be forwarded to and from the phone.

The EtherSwitch network module can connect to a Cisco 7960 IP phone and carry IP voice traffic. If necessary, the EtherSwitch network module can supply electrical power to the circuit connecting it to the Cisco 7960 IP phone.

Because the sound quality of an IP telephone call can deteriorate if the data is unevenly transmitted, the current release of the Cisco IOS software supports QoS based on IEEE 802.1p CoS. QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner.

The Cisco 7960 IP phone contains an integrated three-port 10/100 switch. The ports are dedicated to connect to the following devices:

- Port 1 connects to the EtherSwitch network module switch or other voice-over-IP device
- Port 2 is an internal 10/100 interface that carries the phone traffic
- Port 3 connects to a PC or other device

Port Connection to a Cisco 7960 IP Phone

Because a Cisco 7960 IP phone also supports connection to a PC or other device, a port connecting a EtherSwitch network module to a Cisco 7960 IP phone can carry a mix of traffic. There are three ways to configure a port connected to a Cisco 7960 IP phone:

- All traffic is transmitted according to the default COS priority (0) of the port. This is the default.
- Voice traffic is given a higher priority by the phone, and all traffic is in the same VLAN.
- Voice and data traffic are carried on separate VLANs, and voice traffic always has a CoS priority of 5.

Inline Power on an EtherSwitch Network Module

The EtherSwitch network module can supply inline power to a Cisco 7960 IP phone, if necessary. The Cisco 7960 IP phone can also be connected to an AC power source and supply its own power to the voice circuit. When the Cisco 7960 IP phone is supplying its own power, an EtherSwitch network module can forward IP voice traffic to and from the phone.

A detection mechanism on the EtherSwitch network module determines whether it is connected to a Cisco 7960 IP phone. If the switch senses that there is *no* power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch to never supply power to the Cisco 7960 IP phone and to disable the detection mechanism.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}
5. **power inline** {**auto** | **never**}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot***/***port* Example: `Router(config)# interface fastethernet 1/0`	Selects the port to configure and enters interface configuration mode.

Step 4	**switchport voice vlan** {*vlan*-id | **dot1p** | **none** | **untagged**}
	Example:
	`Router(config-if)# switchport voice vlan dot1p`
		Instructs the EtherSwitch network module to use 802.1p priority tagging for voice traffic and to use VLAN 0 (default native VLAN) to carry all traffic.

Step 5	**power inline** {**auto** | **never**}
	Example:
	`Router(config-if)# power inline never`
		Determine how inline power is applied to the device on the specified port.
		• In this example, inline power on the port is permanently disabled.

Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this step one more time to exit global configuration mode.

Verifying Cisco Discovery Protocol

Perform this optional task to verify that Cisco Discovery Protocol (CDP) is enabled globally, enabled on an interface, and to display information about neighboring equipment. CDP is enabled by default. For more details on CDP commands refer to the *Configuration Fundamentals and Network Management Command Reference*, Release 12.3 T.

SUMMARY STEPS

1. **enable**
2. **show cdp**
3. **show cdp interface** [*interface-type interface-number*]
4. **show cdp neighbors** [*interface-type interface-number*] [**detail**]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show cdp**

Use this command to verify that CDP is globally enabled:

```
Router# show cdp

Global CDP information:
        Sending CDP packets every 120 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

Step 3 **show cdp interface** [*interface-type interface-number*]

Use this command to verify the CDP configuration on an interface:

```
Router# show cdp interface fastethernet 5/1

FastEthernet5/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 120 seconds
  Holdtime is 180 seconds
```

Step 4 **show cdp neighbors** [*interface-type interface-number*] [**detail**]

Use this command to verify information about the neighboring equipment:

```
Router# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
JAB023807H1      Fas 5/3            127         T S       WS-C2948  2/46
JAB023807H1      Fas 5/2            127         T S       WS-C2948  2/45
JAB023807H1      Fas 5/1            127         T S       WS-C2948  2/44
JAB023807H1      Gig 1/2            122         T S       WS-C2948  2/50
JAB023807H1      Gig 1/1            122         T S       WS-C2948  2/49
JAB03130104      Fas 5/8            167         T S       WS-C4003  2/47
JAB03130104      Fas 5/9            152         T S       WS-C4003  2/48
```

Configuring the MAC Table to Provide Port Security

Perform this task to enable the MAC address secure option, create a static or dynamic entry in the MAC address table, and configure the aging timer.

Port security is implemented by providing the user with the option to make a port secure by allowing only well-known MAC addresses to send in data traffic.

MAC Addresses and VLANs

The EtherSwitch network module uses the MAC address tables to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include the following types of addresses:

- Dynamic address—a source MAC address that the switch learns and then drops when it is not in use.
- Secure address—a manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
- Static address—a manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address.

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. Use the Aging Time field to define how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Caution Cisco advises that you do not change the aging timer because the EtherSwitch network module could go out of synchronization.

Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

You can enter a secure port address even when the port does not yet belong to a VLAN. When the port is later assigned to a VLAN, packets destined for that address are forwarded to the port.

Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map. A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac-address-table secure** *mac-address* {**fastethernet | gigabitethernet**} *slot***/***port* **vlan** *vlan-id*
4. **mac-address-table** [**dynamic** | **static**] *mac-address* {**fastethernet | gigabitethernet}** *slot***/***port* **vlan** *vlan-id*

5. **mac-address-table aging-time** *seconds*
6. **exit**
7. **show mac-address-table** [**aging-time** | **secure**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**mac-address-table secure** *mac-address* {**fastethernet** | **gigabitethernet**} *slot***/***port* **vlan** *vlan-id* **Example:** `Router(config)# mac-address-table secure 0003.0003.0003 fastethernet 2/8 vlan 2`	Secures the MAC address traffic on the port. • Use the **no** form of this command to restore the defaults.
Step 4	**mac-address-table** [**dynamic** | **static**] *mac-address* {**fastethernet** | **gigabitethernet**} *slot***/***port* ***vlan*** *vlan-id* **Example:** `Router(config)# mac-address-table static 0001.6443.6440 fastethernet 2/8 vlan 1`	Creates a static or dynamic entry in the MAC address table. **Note** Only the port where the link is up will see the dynamic entry validated in the EtherSwitch network module.
Step 5	**mac-address-table aging-time** *seconds* **Example:** `Router(config)# mac-address-table aging-timer 23`	Configures the MAC address aging-timer age in seconds. • Default aging time is 300 seconds.

Step 6	`exit`
	Example:
	`Router(config-if)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Step 7	**show mac-address-table** [**aging-time** | **secure**] **Example:** `Router# show mac-address-table secure`	(Optional) Displays information about the MAC address table.

Examples

Sample Output for the show mac-address-table Command

In the following example, output information is displayed to verify the configuration of the secure port:

```
Router# show mac-address-table secure

Secure Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0003.0003.0003          Secure 1  FastEthernet    2/8
```

In the following example, information about static and dynamic addresses in the MAC address table is displayed:

```
Router# show mac-address-table

Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0001.6443.6440          Static       1      Vlan1
0004.c16d.9be1          Dynamic      1      FastEthernet2/13
0004.ddf0.0282          Dynamic      1      FastEthernet2/13
0006.0006.0006          Dynamic      1      FastEthernet2/13
001b.001b.ad45          Dynamic      1      FastEthernet2/13
```

In the following example, information about the MAC address aging timer is displayed:

```
Router# show mac-address-table aging-timer

Mac address aging time 23
```

Configuring 802.1x Authentication

Perform the following tasks to configure 802.1x port-based authentication on the EtherSwitch network module:

- Enabling 802.1x Authentication, page 145 (required)
- Configuring the Switch-to-RADIUS-Server Communication, page 147 (optional)
- Configuring 802.1x Parameters (Retransmissions and Timeouts), page 148 (optional)

802.1x Authentication Guidelines for the EtherSwitch network module

These are the 802.1x authentication configuration guidelines:

- When the 802.1x protocol is enabled, ports are authenticated before any other Layer 2 feature is enabled.
- The 802.1x protocol is supported on Layer 2 static-access ports, but it is not supported on these port types:
  - Trunk port—If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.

- EtherChannel port—Before enabling 802.1x on the port, you must first remove the port from the EtherChannel before enabling 802.1x on it. If you try to enable 802.1x on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1x is not enabled. If you enable 802.1x on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

Switch Port Analyzer (SPAN) destination port—You can enable 802.1x on a port that is a SPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. You can enable 802.1x on a SPAN source port.

Table 13 shows the default 802.1x configuration.

Table 13 Default 802.1x Configuration

Feature	Default Setting
Authentication, authorization, and accounting (AAA)	Disabled.
RADIUS server • IP address • UDP authentication port • Key	 • None specified. • 1645. • None specified.
Per-interface 802.1x enable state	Disabled (force-authorized). The port transmits and receives normal traffic without 802.1x-based authentication of the client.
Periodic reauthentication	Disabled.
Number of seconds between reauthentication attempts	3600 seconds.
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).
Retransmission time	30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request).
Maximum retransmission number	2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).
Multiple host support	Disabled.
Client timeout period	30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before retransmitting the request to the client). This setting is not configurable.
Authentication server timeout period	30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before retransmitting the response to the server). This setting is not configurable.

Enabling 802.1x Authentication

To enable 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

You control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized**—disables 802.1x and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
- **force-unauthorized**—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
- **auto**—enables 802.1x and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up, or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address.

To disable AAA, use the **no aaa new-model** global configuration command. To disable 802.1x AAA authentication, use the **no** form of the **aaa authentication dot1x** global configuration command. To disable 802.1x, use the **dot1x port-control** command with the **force-authorized** keyword or the **no** form of the **dot1x port-control** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication dot1x default group radius**
5. **interface** *type slot*/*port*
6. **dot1x port-control** [**auto** | **force-authorized** | **force-unauthorized**]
7. **exit**

DETAILED STEPS

	Command	Description

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`aaa new-model`**
	Example:
	`Router (config)# aaa new-model`
		Enables AAA.

Step 4	**`aaa authentication dot1x default group radius`**
	Example:
	`Router (config)# aaa authentication dot1x default group radius`
		Creates an 802.1x authentication method list.
		To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.
		Enter at least one of these keywords:
		• **group radius**—Use the list of all RADIUS servers for authentication.
		• **none**—Use no authentication. The client is automatically authenticated without the switch using the information supplied by the client.

Step 5	**`interface`** *`type slot`*`/`*`port`*
	Example:
	`Router (config)# interface fastethernet 5/1`
		Enters interface configuration mode and specifies the interface to be enabled for 802.1x port-based authentication.

Step 6	**`dot1x port-control`** `[`**`auto`** `|` **`force-authorized`** `|` **`force-unauthorized`**`]`
	Example:
	`Router (config-if)# dot1x port-control auto`
		Enables 802.1x port-based authentication on the interface.
		For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports, see the "802.1x Authentication Guidelines for the EtherSwitch network module" section on page 143.

Step 7	**`exit`**
	Example:
	`Router(config)# exit`
		Exits interface configuration mode and returns the router to privileged EXEC mode.
		• Repeat this command to exit global configuration mode and return to privileged EXEC mode.

Configuring the Switch-to-RADIUS-Server Communication

Perform this task to configure RADIUS server parameters.

RADIUS Security Servers

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*
5. **radius-server key** *string*

DETAILED STEPS

	Command	Description

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ip radius source-interface`** *`interface-name`*
	Example:
	`Router (config)# ip radius source-interface ethernet1`
		Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

	Command	Description

Step 4	**`radius-server host`** {*`hostname`* | *`ip-address`*} **`auth-port`** *`port-number`* **`key`** *`string`*
	Example:
	`Router (config)# radius-server host 172.16.39.46 auth-port 1612 key rad123`
		Configures the RADIUS server parameters on the switch.
		• Use the *hostname* or *ip-address* argument to specify the host name or IP address of the remote RADIUS server.
		• Use the **auth-port** *port-number* keyword and argument to specify the UDP destination port for authentication requests. The default is 1645.
		• Use the **key** *string* keyword and argument to specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.
		Note Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.
		• To use multiple RADIUS servers, repeat this command for each server.

Step 5	**`radius-server key`** *`string`*
	Example:
	`Router (config)# radius-server key radiuskey`
		Configures the authorization and encryption key used between the router and the RADIUS daemon running on the RADIUS server.
		• The key is a text string that must match the encryption key used on the RADIUS server.

Configuring 802.1x Parameters (Retransmissions and Timeouts)

Perform this task to configure various 802.1x retransmission and timeout parameters. Because all of these parameters have default values, configuring them is optional.

Note You should change the default values of these commands only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*

4. **dot1x port-control** [**auto** | **force-authorized** | **force-unauthorized**]
5. **dot1x multiple-hosts**
6. **exit**
7. **dot1x max-req** *number-of-retries*
8. **dot1x re-authentication**
9. **dot1x timeout tx-period** *value*
10. **dot1x timeout re-authperiod** *value*
11. **dot1x timeout quiet-period** *value*
12. **dot1x default**
13. **exit**
14. **show dot1x** [**statistics**] [**interface** *interface-type interface-number*]

DETAILED STEPS

	Command	Description

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface {ethernet | fastethernet | gigabitethernet} slot/port`
	Example:
	`Router(config)# interface fastethernet 5/6`
		Specifies the interface to which multiple hosts are indirectly attached and enters interface configuration mode.

Step 4	`dot1x port-control [auto | force-authorized | force-unauthorized]`
	Example:
	`Router (config-if)# dot1x port-control auto`
		Enables 802.1x port-based authentication on the interface.
		For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports, see the "802.1x Authentication Guidelines for the EtherSwitch network module" section on page 143.

Step 5	**`dot1x multiple-hosts`**
	Example:
	`Router (config-if)# dot1x multiple-hosts`
		Allows multiple hosts (clients) on an 802.1x-authorized port.
		Note Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.

	Command	Description
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode.
Step 7	**dot1x max-req** *number-of-retries* **Example:** `Router (config)# dot1x max-req 3`	Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. • The range is from 1 to 10; the default is 2.
Step 8	**dot1x re-authentication** **Example:** `Router (config)# dot1x reauthentication`	Enables periodic reauthentication of the client, which is disabled by default. • The reauthentication period can be set using the **dot1x timeout** command.
Step 9	**dot1x timeout re-authperiod** *value* **Example:** `Router (config)# dot1x timeout re-authperiod 1800`	Sets the number of seconds between reauthentication attempts. • The range is from 1 to 4294967295; the default is 3600 seconds. **Note** This command affects the behavior of the switch only if periodic reauthentication is enabled.
Step 10	**dot1x timeout tx-period** *value* **Example:** `Router (config)# dot1x timeout tx-period 60`	Sets the number of seconds that the EtherSwitch network module waits for a response to an EAP-request/identity frame from the client before retransmitting the request. • The range is from 1 to 65535 seconds; the default is 30.
Step 11	**dot1x timeout quiet-period** *value* **Example:** `Router (config)# dot1x timeout quiet-period 600`	Sets the number of seconds that the EtherSwitch network module remains in a quiet state following a failed authentication exchange with the client. • The range is from 1 to 65535 seconds; the default is 60.
Step 12	**dot1x default** **Example:** `Router (config)# dot1x default`	Resets the configurable 802.1x parameters to the default values.
Step 13	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 14	**show dot1x** [**statistics**] [**interface** *interface-type interface-number*] **Example:** `Router# show dot1x statistics interface fastethernet 0/1`	(Optional) Displays 802.1x statistics, administrative status, and operational status for the EtherSwitch network module or a specified interface.

Examples

Sample Output for the show dot1x Command

In the following example, statistics appear for all the physical ports for the specified interface:

```
Router# show dot1x statistics fastethernet 0/1

FastEthernet0/1

    Rx: EAPOL     EAPOL     EAPOL     EAPOL     EAP       EAP       EAP
        Start     Logoff    Invalid   Total     Resp/Id   Resp/Oth  LenError
        0         0         0         21        0         0         0

        Last      Last
        EAPOLVer  EAPOLSrc
        1         0002.4b29.2a03

    Tx: EAPOL     EAP       EAP
        Total     Req/Id    Req/Oth
        622       445       0
```

In the following example, global 802.1x parameters and a summary are displayed:

```
Router# show dot1x

Global 802.1X Parameters
    reauth-enabled                no
    reauth-period               3600
    quiet-period                  60
    tx-period                     30
    supp-timeout                  30
    server-timeout                30
    reauth-max                     2
    max-req                        2

802.1X Port Summary
    Port Name                Status      Mode                Authorized
    Gi0/1                    disabled    n/a                 n/a
    Gi0/2                    enabled     Auto (negotiate)    no

802.1X Port Details
    802.1X is disabled on GigabitEthernet0/1
802.1X is enabled on GigabitEthernet0/2
      Status                Unauthorized
      Port-control          Auto
      Supplicant            0060.b0f8.fbfb
      Multiple Hosts        Disallowed
      Current Identifier    2

      Authenticator State Machine
        State               AUTHENTICATING
        Reauth Count        1

      Backend State Machine
        State               RESPONSE
        Request Count       0
        Identifier (Server) 2

      Reauthentication State Machine
        State               INITIALIZE
```

Configuring Power Management on the Interfaces

Perform this task to manage the powering of the Cisco IP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **power inline** {**auto** | **never**}
5. **exit**
6. **show power inline**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port* **Example:** `Router(config)# interface fastethernet 5/6`	Selects the Ethernet interface to configure and enters interface configuration mode.

Step 4	**power inline** {**auto** | **never**}
	Example:
	`Router(config-if)# power inline auto`
		Configures the port to supply inline power automatically to a Cisco IP phone.
		• Use the **never** keyword to permanently disable inline power on the port.

Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this command to exit global configuration mode and return to privileged EXEC mode.
Step 6	**show power inline** **Example:** `Router# show power inline`	(Optional) Displays information about the power configuration on the ports.

Examples

Sample Output for the show power inline Command

In the following example, output information is displayed to verify the power configuration on the ports:

```
Router# show power inline

PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
 EXT-PS          1       165.000    20.000         PS1 GOOD PS2 ABSENT

Interface           Config   Phone     Powered    PowerAllocated
---------           ------   -----     -------    --------------
FastEthernet1/0      auto    no           off      0.000 Watts
FastEthernet1/1      auto    no           off      0.000 Watts
FastEthernet1/2      auto    no           off      0.000 Watts
FastEthernet1/3      auto    no           off      0.000 Watts
FastEthernet1/4      auto    unknown      off      0.000 Watts
FastEthernet1/5      auto    unknown      off      0.000 Watts
FastEthernet1/6      auto    unknown      off      0.000 Watts
FastEthernet1/7      auto    unknown      off      0.000 Watts
FastEthernet1/8      auto    unknown      off      0.000 Watts
FastEthernet1/9      auto    unknown      off      0.000 Watts
FastEthernet1/10     auto    unknown      off      0.000 Watts
FastEthernet1/11     auto    yes          on       6.400 Watts
FastEthernet1/12     auto    yes          on       6.400 Watts
FastEthernet1/13     auto    no           off      0.000 Watts
FastEthernet1/14     auto    unknown      off      0.000 Watts
FastEthernet1/15     auto    unknown      off      0.000 Watts
```

Configuring Storm Control

This section consists of two tasks. The first task enables global storm control, and the second task configures storm control on a per-port basis.

- Enabling Global Storm Control, page 153
- Enabling Per-Port Storm Control, page 155

Enabling Global Storm Control

Perform this task to enable a specified type of global storm control.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **storm-control** {{{**broadcast** | **multicast** | **unicast**} **level** *level* [*lower-level*]} | **action shutdown**}
4. **exit**
5. **show interface** [*interface-type interface-number*] **counters** {**broadcast** | **multicast** | **unicast**}

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`storm-control`** `{{{`**`broadcast`** `|` **`multicast`** `|` **`unicast`**`}` **`level`** *`level`* `[`*`lower-level`*`]}|` **`action shutdown`**`}`
	Example:
	`Router(config)# storm-control broadcast level 75`
		Specifies the global broadcast, multicast, or unicast storm control suppression level as a percentage of total bandwidth.
		- A threshold value of 100 percent means that no limit is placed on the specified type of traffic.
		- Use the **level** keyword and argument to specify the threshold value.
		- Use the **no** form of this command to restore the defaults.

Step 4	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode and returns the router to global configuration mode.
		- Repeat this command to exit global configuration mode and return to privileged EXEC mode.

Step 5	**`show interface`** `[`*`interface-type interface-number`*`]` **`counters`** `{`**`broadcast`** `|` **`multicast`** `|` **`unicast`**`}`
	Example:
	`Router# show interface counters broadcast`
		(Optional) Displays the type of storm control suppression counter currently in use and displays the number of discarded packets.
		- Use the *interface-type* and *interface-number* arguments to display the type of storm control suppression counter for a specified interface.

Examples

Sample Output for the show interface counters Command

In the following example, output information is displayed to verify the number of packets discarded for the specified storm control suppression:

```
Router# show interface counters broadcast

Port      BcastSuppDiscards
Fa0/1                     0
Fa0/2                     0
```

Enabling Per-Port Storm Control

Perform this task to configure storm control on a specified interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **storm-control** {{{**broadcast** | **multicast** | **unicast**} **level** *level* [*lower-level*]} | **action shutdown**}
5. **storm-control action shutdown**
6. **exit**
7. **show storm-control** [*interface-type interface-number*] [**broadcast** | **multicast** | **unicast** | **history**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port* **Example:** `Router(config)# interface fastethernet 5/6`	Selects the Ethernet interface to configure and enters interface configuration mode.

Step 4	**storm-control** {{{**broadcast** | **multicast** | **unicast**} **level** *level* [*lower-level*]}| **action shutdown**}
	Example:
	`Router(config-if)# storm-control multicast level 80`
		Configures broadcast, multicast, or unicast per-port storm-control.
		• Use the **level** keyword and argument to specify the rising threshold level for either broadcast, multicast, or unicast traffic. The storm control action occurs when traffic utilization reaches this level.
		• Use the optional *lower-level* argument to specify the falling threshold level. The normal transmission restarts (if the action is filtering) when traffic drops below this level.
		• A threshold value of 100 percent means that no limit is placed on the specified type of traffic.
		• Use the **no** form of this command to restore the defaults.

	Command or Action	Purpose

Step 5	**`storm-control action shutdown`**
	Example:
	`Router(config-if)# storm-control action shutdown`
		Selects the **shutdown** keyword to disable the port during a storm.
		• The default is to filter out the traffic
		• Use the **no** keyword to restore the defaults.

Step 6	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode and returns the router to global configuration mode.
		• Repeat this command to exit global configuration mode and return to privileged EXEC mode.

Step 7	**`show storm-control`** [*`interface-type interface-number`*] [**`broadcast`** | **`multicast`** | **`unicast`** | **`history`**] **Example:** `Router# show storm-control broadcast`	(Optional) Displays the type of storm control suppression for all interfaces on the EtherSwitch network module. • Use the *interface-type* and *interface-number* arguments to display the type of storm control suppression for a specified interface.

Examples

Sample Output for the show storm-control Command

In the following example, output information is displayed to verify the number of packets discarded for the specified storm control suppression:

```
Router# show storm-control broadcast

Interface  Filter State   Upper    Lower    Current
---------  -------------  -------  -------  -------
Fa0/1      <inactive>     100.00%  100.00%    0.00%
Fa0/2      <inactive>     100.00%  100.00%    0.00%
Fa0/3      <inactive>     100.00%  100.00%    0.00%
Fa0/4      Forwarding      30.00%   20.00%   20.32%
```

Configuring Layer 2 EtherChannels (Port-Channel Logical Interfaces)

Perform this task to configure Layer 2 Ethernet interfaces as a Layer 2 EtherChannel, configure EtherChannel load balancing, and remove an Ethernet interface from an EtherChannel.

To configure Layer 2 EtherChannels, configure the Ethernet interfaces with the **channel-group** command, which creates the port-channel logical interface. You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

Restrictions

- Cisco IOS software creates port-channel interfaces for Layer 2 EtherChannels when you configure Layer 2 Ethernet interfaces with the **channel-group** command. You cannot put Layer 2 Ethernet interfaces into a manually created port-channel interface.
- Layer 2 interfaces must be connected and functioning for Cisco IOS software to create port-channel interfaces for Layer 2 EtherChannels.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **channel-group** *port-channel-number* **mode on**
5. Repeat Steps 3 through 4 for each Ethernet interface to be added as a Layer 2 EtherChannel.
6. **exit**
7. **port-channel load-balance** {**src-mac** | **dst-mac** | **src-dst-mac** | **src-ip** | **dst-ip** | **src-dst-ip**}
8. **no interface port-channel** *port-channel-number*
9. **exit**
10. **show interfaces fastethernet** *slot*/*port* {**etherchannel** | **switchport** | **trunk**}
11. **show etherchannel** [*channel-group*] {**port-channel** | **brief** | **detail** | **summary** | **port** | **load-balance**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port* **Example:** `Router(config)# interface fastethernet 5/6`	Selects the Ethernet interface to configure.
Step 4	**channel-group** *port-channel-number* **mode on** **Example:** `Router(config)# channel-group 2 mode on`	Configures the interface in a port-channel. • In this example, the Etherchannel group 2 is configured.
Step 5	Repeat Steps 3 through 4 for each Ethernet interface to be added as a Layer 2 EtherChannel.	—
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode.

	Command or Action	Purpose

Step 7	**port-channel load-balance** {**src-mac** | **dst-mac** | **src-dst-mac** | **src-ip** | **dst-ip** | **src-dst-ip**}
	Example:
	`Router(config)# port-channel load-balancing src-mac`
		Configures EtherChannel load balancing.
		• In this example, the load balancing is based on the source MAC addresses.

Step 8	**no interface port-channel** *port-channel-number* **Example:** `Router(config)# no interface port-channel 3`	Removes a port channel interface. • In this example, the interface port channel 3 is removed.
Step 9	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.

Step 10	**show interfaces fastethernet** *slot*/*port* {**etherchannel** | **switchport** | **trunk**}
	Example:
	`Router# show interfaces fastethernet 5/6 etherchannel`
		(Optional) Displays information about Fast Ethernet interfaces.
		• In this example, EtherChannel information is shown for the specified interface.

Step 11	**show etherchannel** [*channel-group*] {**port-channel** | **brief** | **detail** | **summary** | **port** | **load-balance**}
	Example:
	`Router# show etherchannel 2 port-channel`
		(Optional) Displays information about port channels for EtherChannel groups.

Examples

Sample Output for the show interfaces fastethernet Command

In the following example, output information is displayed to verify the configuration of Fast Ethernet interface as a Layer 2 EtherChannel:

```
Router# show interfaces fastethernet 5/6 etherchannel

Port state    = EC-Enbld Up In-Bndl Usr-Config

Channel group = 2           Mode = Desirable     Gcchange = 0
Port-channel  = Po2         GC   = 0x00020001
Port indx     = 1           Load = 0x55

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Local information:
                                Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Fa5/6     SC    U6/S7           30s      1        128        Any      56

Partner's information:
```

```
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Fa5/6     JAB031301            0050.0f10.230c   2/47        18s SAC     2F

Age of the port in the current state: 00h:10m:57s
```

Sample Output for the show etherchannel Command

In the following example, output information about port channels for EtherChannel group 2 is displayed:

```
Router# show etherchannel 2 port-channel

Port-channels in the group:
                ----------------------

Port-channel: Po2
------------

Age of the Port-channel   = 00h:23m:33s
Logical slot/port   = 10/2           Number of ports in agport = 2
GC                  = 0x00020001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse

Ports in the Port-channel:

Index   Load   Port
-------------------
  1     55      Fa5/6
  0     AA      Fa5/7

Time since last port bundled:    00h:23m:33s    Fa5/6
```

Configuring Flow Control on Gigabit Ethernet Ports

Perform this task to configure flow control on a Gigabit Ethernet port.

SUMMARY STEPS

1. **enable**
2. **set port flowcontrol** {**receive** | **send**} [*mod-number*/*port-number*] {**off** | **on** | **desired**}
3. **show port flowcontrol**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`set port flowcontrol`** `{`**`receive`** `|` **`send`**`}` `[`*`mod-number/port-number`*`]` `{`**`off`** `|` **`on`** `|` **`desired`**`}`
	Example:
	`Router# set port flowcontrol 5/1 receive on`
		Sets the flow control parameters on a Gigabit Ethernet port.

Step 3	**`show port flowcontrol`**
	Example:
	`Router# show port flowcontrol`
		(Optional) Displays information about the flow control for Gigabit Ethernet ports.

Examples

Sample Output for the show port flowcontrol Command

In the following example, output information is displayed to verify the flow control configuration on Gigabit Ethernet ports:

```
Router# show interfaces fastethernet 5/6 etherchannel

Port   Send-Flowcontrol   Receive-Flowcntl   RxPause   TxPause
       Admin   Oper       Admin   Oper
-----  ----------------   ----------------   -------   ------
 5/1   off     off        on      disagree   0         0
 5/2   off     off        off     off        0         0
 5/3   desired on         desired off        10        10
```

Configuring Intrachassis Stacking

Perform this task to extend Layer 2 switching in the router by connecting the Gigabit Ethernet ports of the EtherSwitch network module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/port*
4. **switchport stacking-partner interface gigabit** *slot/port*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface gigabitethernet`** *`slot`*`/`*`port`*
	Example:
	`Router(config)# interface gigabitethernet 2/0`
		Selects the Gigabit Ethernet interface to configure.

Step 4	**`switchport stacking-partner interface gigabitethernet`** *`slot`*`/`*`port`*
	Example:
	`Router(config-if)# switchport stacking-link interface gigabitethernet 3/0`
		Creates the intrachassis stacking between the current Gigabit Ethernet (GE) interface and the stacking link partner GE interface.
		• In this example, GE interface 2/0 is stacked on GE interface 3/0 to form an extended VLAN within one chassis on the router.

Step 5	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode and returns the router to global configuration mode.
		• Repeat this command to exit global configuration mode and return to privileged EXEC mode.

Configuring Switched Port Analyzer (SPAN)

Perform this task to configure the source and destination for a SPAN session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *session-number* {**source interface** *interface-type slot*/*port* | **vlan** *vlan-id*} [**,** | **-** | **rx** | **tx** | **both**]
4. **monitor session** *session-number* {**destination interface** *interface-type slot*/*port* [**,** | **-**] | **vlan** *vlan-id*}
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *session-number* {**source interface** *interface-type slot*/*port* | **vlan** *vlan-id*} [**,** | **-** | **rx** | **tx** | **both**] **Example:** `Router(config)# monitor session 1 source interface fastethernet 5/1 both`	Specifies the SPAN session number, the source interface, or VLAN, and the traffic direction to be monitored. **Note** Multiple SPAN sessions can be configured, but only one SPAN session is supported at a time.

Step 4	**monitor session** *session-number* {**destination interface** *interface-type slot*/*port* [**,** | **-**] | **vlan** *vlan-id*}
	Example:
	`Router(config)# monitor session 1 destination interface fastethernet 5/48`
		Specifies the SPAN session number, the destination interface, or VLAN.

Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.

Configuring Layer 3 Interfaces

Perform this task to configure a Layer 3 interface on the EtherSwitch network module. A physical interface on the EtherSwitch network module is configured as a Layer 3 interface and an IP address is assigned to the interface.

Layer 3 Interface Support for the EtherSwitch network module

The EtherSwitch network module supports two types of Layer 3 interfaces for routing and bridging:

- SVIs: You should configure SVIs for any VLANs for which you want to route traffic. SVIs are created when you enter a VLAN ID following the **interface vlan** global configuration command. To delete an SVI, use the **no interface vlan** global configuration command.
- Routed ports: Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.

Note A Layer 3 switch can have an IP address assigned to each routed port and SVI. The number of routed ports and SVIs that you can configure is not limited by software; however, the interrelationship between this number and the number of other features being configured might have an impact on CPU utilization because of hardware limitations.

All Layer 3 interfaces require an IP address to route traffic (a routed port cannot obtain an IP address from a DHCP server, but the router can act as a DHCP server and serve IP addresses through a routed port).

Routed ports support only CEF switching (IP fast switching is not supported).

Note If the physical port is in Layer 2 mode (the default), you must enter the **no switchport** interface configuration command to put the interface into Layer 3 mode. Entering a **no switchport** command disables and then reenables the interface, which might generate messages on the device to which the interface is connected. When you use this command to put the interface into Layer 3 mode, you are also deleting any Layer 2 characteristics configured on the interface. (Also, when you return the interface to Layer 2 mode, you are deleting any Layer 3 characteristics configured on the interface.)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **no switchport**
5. **ip address** *ip-address mask*
6. **no shutdown**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface`** `{`**`ethernet`** `|` **`fastethernet`** `|` **`gigabitethernet`**`}` *`slot`*`/`*`port`*
	Example:
	`Router(config)# interface gigabitethernet 0/10`
		Selects the Ethernet interface to configure.

	Command or Action	Purpose

Step 4	`no switchport`
	Example:
	`Router(config-if)# no switchport`
		Disables switching on the port and enables routing (Layer 3) mode for physical ports only.
		• In this example, Gigabit Ethernet interface 0/10 is now a routed port instead of a switching port.

Step 5	**`ip address`** *`ip-address mask`*
	Example:
	`Router(config)# ip address 10.1.2.3 255.255.0.0`
		Configures an IP address and subnet.

Step 6	`no shutdown`
	Example:
	`Router(config-if)# no shutdown`
		Activates the interface. (Required only if you shut down the interface.)

Step 7	`exit`
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode and returns the router to global configuration mode.
		• Repeat this command to exit global configuration mode and return to privileged EXEC mode.

Enabling and Verifying IP Multicast Layer 3 Switching

Perform this task to enable IP multicast routing globally, enable IP Protocol Independent Multicast (PIM) on a Layer 3 interface, and verify the IP multicast Layer 3 switching information.

You must enable IP multicast routing globally before enabling IP multicast Layer 3 switching on Layer 3 interfaces. Enable PIM on Layer 3 interfaces before adding IP multicast Layer 3 switching functions on those interfaces.

For complete IP multicast command reference information and configuration details, refer to the following documents:

- *Cisco IOS IP Configuration Guide*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*, Release 12.3 T

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**
4. **interface vlan** *vlan-id*
5. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}
6. **exit**
7. **show ip pim** [**vrf** *vrf-name*] **interface** [*interface-type interface-number*] [**df** | **count**] [*rp-address*] [**detail**]
8. **show ip mroute** [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**ip multicast-routing**
	`Example:`
	`Router(config)# ip multicast-routing`
		Enables IP multicast routing globally.

Step 4	**interface vlan** *vlan-id* **Example:** `Router(config)# interface vlan 10`	Selects the interface to configure.

Step 5	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}
	`Example:`
	`Router(config-if)# ip pim sparse-mode`
		Enables IP PIM on a Layer 3 interface.

Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this command to exit global configuration mode and return to privileged EXEC mode.
Step 7	**show ip pim** [**vrf** *vrf-name*] **interface** [*interface-type interface-number*] [**df** | **count**] [*rp-address*] [**detail**] **Example:** `Router# show ip pim interface count`	Verifies the IP multicast Layer 3 switching enable state on IP PIM interfaces. • Use the **count** keyword to display the number of packets received and sent on the interface.
Step 8	**show ip mroute** [**vrf** *vrf-name*] [group-address | *group-name*] [source-address | source-*name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `Router# show ip mroute count`	Displays the contents of the IP multicast routing (mroute) table.

Examples

Sample Output for the show ip pim Command

In the following example, output information is displayed to verify the IP multicast Layer 3 switching information for an IP PIM Layer 3 interface:

```
Router# show ip pim interface count

State:* - Fast Switched, D - Distributed Fast Switched
      H - Hardware Switching Enabled
Address          Interface          FS  Mpackets In/Out
10.15.1.20       GigabitEthernet4/8 * H 952/4237130770
10.20.1.7        GigabitEthernet4/9 * H 1385673757/34
10.25.1.7        GigabitEthernet4/10* H 0/34
10.11.1.30       FastEthernet6/26   * H 0/0
10.37.1.1        FastEthernet6/37   * H 0/0
1.22.33.44       FastEthernet6/47   * H 514/68
```

Sample Output for the show ip mroute Command

In the following example, output information is displayed for the IP multicast routing table:

```
Router# show ip mroute count

IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
  Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
```

Note The negative counter means that the outgoing interface list of the corresponding entry is NULL, and this indicates that this flow is still active.

Configuring IGMP Snooping

Perform this task to enable IGMP snooping on a router with the Ethernet switching network module installed.

IGMP Snooping on the EtherSwitch Network Module

By default, IGMP snooping is globally enabled on the EtherSwitch network module. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. By default, IGMP snooping is enabled on all VLANs, but it can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the per-VLAN IGMP snooping capability. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable snooping on a VLAN basis.

IGMP Immediate-Leave Processing

When you enable IGMP Immediate-Leave processing, the EtherSwitch network module immediately removes a port from the IP multicast group when it detects an IGMP version 2 leave message on that port. Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out group-specific queries to the interface. You should use the Immediate-Leave feature only when there is only a single receiver present on every port in the VLAN.

Static Configuration of an Interface to Join a Multicast Group

Ports normally join multicast groups through the IGMP report message, but you can also statically configure a host on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping**
4. **ip igmp snooping vlan** *vlan-id*
5. **ip igmp snooping vlan** *vlan-id* **immediate-leave**
6. **ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-type slot***/***port*
7. **ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-type slot***/***port* **|** **learn pim-dvmrp**}
8. **exit**
9. **show ip igmp snooping** [**vlan** *vlan-id*]
10. **show ip igmp snooping mrouter** [**vlan** *vlan-id*]
11. **show mac-address-table multicast** [**vlan** *vlan-id*] [**user** **|** **igmp-snooping**] [**count**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ip igmp snooping`**
	Example:
	`Router(config)# ip igmp snooping`
		Globally enables IGMP snooping on all existing VLAN interfaces.

Step 4	**`ip igmp snooping vlan`** *`vlan-id`*
	Example:
	`Router(config)# ip igmp snooping vlan 10`
		Enables IGMP snooping on the specified VLAN interface.

Step 5	**`ip igmp snooping vlan`** *`vlan-id`* **`immediate-leave`**
	Example:
	`Router(config)# ip igmp snooping vlan 10 immediate-leave`
		Enables IGMP Immediate-Leave processing on the specified VLAN interface.

	Command or Action	Purpose
Step 6	**ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-type slot***/***port* **Example:** `Router(config)# ip igmp snooping vlan 10 static 303.303.303.303 interface fastethernet 1/5`	Statically configures a port as a member of a multicast group: • Use the *vlan-id* argument to specify the multicast group VLAN ID. • Use the *mac-address* argument to specify the group MAC address. • Use the *interface-type* and *slot/port* arguments to configure a port as a member of a multicast group.
Step 7	**ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-type slot***/***port* | **learn pim-dvmrp**} **Example:** `Router(config)# ip igmp snooping vlan 10 mrouter interface fastethernet 1/5`	Enables a static connection on a multicast router. • Use the *vlan-id* argument to specify the multicast group VLAN ID. • Use the *interface-type* and *slot/port* arguments to specify the interface that connects to the multicast router.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 9	**show ip igmp snooping** [**vlan** *vlan-id*] **Example:** `Router# show ip igmp snooping vlan 10`	Displays the IGMP snooping configuration. • Use the *vlan-id* argument to specify the multicast group VLAN ID.
Step 10	**show ip igmp snooping mrouter** [**vlan** *vlan-id*] **Example:** `Router# show ip igmp snooping mrouter vlan 10`	Displays information on dynamically learned and manually configured multicast router interfaces.
Step 11	**show mac-address-table multicast** [**vlan** *vlan-id*] [**user** | **igmp-snooping**] [**count**] **Example:** `Router# show mac-address-table multicast vlan 10 igmp-snooping`	Displays MAC address table entries for a VLAN. • Use the *vlan-id* argument to specify the multicast group VLAN ID. • Use the **user** keyword to display only the user-configured multicast entries. • Use the **igmp-snooping** keyword to display entries learned via IGMP snooping. • Use the **count** keyword to display only the total number of entries for the selected criteria, not the actual entries.

Configuring Fallback Bridging

This section contains the following tasks to help you configure fallback bridging.

- Configuring a Bridge Group, page 169 (required)
- Adjusting Spanning-Tree Parameters, page 172 (optional)
- Disabling the Spanning Tree on an Interface, page 174 (optional)

Understanding the Default Fallback Bridging Configuration

Table 14 shows the default fallback bridging configuration.

Table 14 Default Fallback Bridging Configuration

Feature	Default Setting
Bridge groups	None are defined or assigned to an interface. No VLAN-bridge STP is defined.
Switch forwards frames for stations that it has dynamically learned	Enabled.
Bridge table aging time for dynamic entries	300 seconds.
MAC-layer frame filtering	Disabled.
Spanning tree parameters:	
• Switch priority	• 32768.
• Interface priority	• 128.
• Interface path cost	• 10 Mbps: 100. 100 Mbps: 19. 1000 Mbps: 4.
• Hello BPDU interval	• 2 seconds.
• Forward-delay interval	• 20 seconds.
• Maximum idle interval	• 30 seconds.

Configuring a Bridge Group

Perform this task to create a bridge group, filter frames using a specific MAC address, prevent the forwarding of frames for stations that the switching device has dynamically learned, and remove dynamic entries from the bridge table.

Bridge Group Creation

To configure fallback bridging for a set of SVIs or routed ports, these interfaces must be assigned to bridge groups. All interfaces in the same group belong to the same bridge domain. Each SVI or routed port can be assigned to only one bridge group. A maximum of 31 bridge groups can be configured on the switch.

Note The protected port feature is not compatible with fallback bridging. When fallback bridging is enabled, it is possible for packets to be forwarded from one protected port on a switch to another protected port on the same switch if the ports are in different VLANs.

Forwarding of Dynamically Learned Stations

By default, the switch forwards any frames for stations that it has dynamically learned. By disabling this activity, the switch only forwards frames whose addresses have been statically configured into the forwarding cache.

Bridge Table Aging Time

A switch forwards, floods, or drops packets based on the bridge table. The bridge table maintains both static and dynamic entries. Static entries are entered by you or learned by the switch. Dynamic entries are entered by the bridge learning process. A dynamic entry is automatically removed after a specified length of time, known as aging time, from the time the entry was created or last updated.

If you are likely to move hosts on a switched network, decrease the aging-time to enable the switch to quickly adapt to the change. If hosts on a switched network do not continuously send packets, increase the aging time to keep the dynamic entries for a longer time and thus reduce the possibility of flooding when the hosts send again.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **protocol vlan-bridge**
4. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
5. **bridge-group** *bridge-group*
6. **exit**
7. **bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-type interface-number*]
8. **no bridge** *bridge-group* **acquire**
9. **bridge** *bridge-group* **aging-time** *seconds*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bridge** *bridge-group* **protocol vlan-bridge** **Example:** `Router(config)# bridge 10 protocol vlan-bridge`	Assigns a bridge group number, and specifies the VLAN-bridge spanning-tree protocol to run in the bridge group. • Use the *bridge-group* argument to specify the bridge group number. The range is 1 to 255. You can create up to 31 bridge groups. **Note** Frames are bridged only among interfaces in the same group.

	Command or Action	Purpose
Step 4	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port* **Example:** `Router(config)# interface gigabitethernet 0/1`	Selects the Ethernet interface on which the bridge group is assigned and enters interface configuration mode. The specified interface must be one of the following: • A routed port: a physical port that you have configured as a Layer 3 port by entering the **no switchport** interface configuration command. • An SVI: a VLAN interface that you created by using the **interface vlan** *vlan-id* global configuration command. **Note** These ports must have IP addresses assigned to them.
Step 5	**bridge-group** *bridge-group* **Example:** `Router(config-if)# bridge-group 10`	Assigns the interface to the bridge group created in Step 3. • By default, the interface is not assigned to any bridge group. • An interface can be assigned to only one bridge group.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode.
Step 7	**bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-type interface-number*] **Example:** `Router(config)# bridge 1 address 0800.cb00.45e9 forward gigabitethernet 0/1`	Specifies the MAC address to discard or forward. • Use the *bridge-group* argument to specify the bridge group number. The range is from 1 to 255. • Use the **address** *mac-address* keyword and argument to specify the MAC-layer destination address to be filtered. • Use the **forward** keyword if you want the frame destined to the specified interface to be forwarded. Use the **discard** keyword if you want the frame to be discarded. • (Optional) Use the *interface-type* and *interface-number* arguments to specify the interface on which the address can be reached.
Step 8	**no bridge** *bridge-group* **acquire** **Example:** `Router(config-if)# no bridge 10 acquire`	Stops the EtherSwitch network module from forwarding any frames for stations that it has dynamically learned through the discovery process, and to limit frame forwarding to statically configured stations. • The switch filters all frames except those whose destined-to addresses have been statically configured into the forwarding cache. • To configure a static address, use the **bridge address** global configuration command, see Step 7. • Use the *bridge-group* argument to specify the bridge group number. The range is from 1 to 255.

	Command or Action	Purpose
Step 9	**bridge** *bridge-group* **aging-time** *seconds* **Example:** `Router(config-if)# bridge 10 aging-time 200`	Specifies the length of time that a dynamic entry remains in the bridge table from the time the entry was created or last updated. • Use the *bridge-group* argument to specify the bridge group number. The range is from 1 to 255. • Use the *second*s argument to enter a number from 0 to 1000000. The default is 300.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.

Adjusting Spanning-Tree Parameters

Perform this task to adjust spanning tree parameters such as the switch priority or interface priority. You might need to adjust certain spanning-tree parameters if the default values are not suitable for your switch configuration. Parameters affecting the entire spanning tree are configured with variations of the **bridge** global configuration command. Interface-specific parameters are configured with variations of the **bridge-group** interface configuration command.

Note Only network administrators with a good understanding of how switches and STP function should make adjustments to spanning-tree parameters. Poorly planned adjustments can have a negative impact on performance. A good source on switching is the IEEE 802.1d specification; for more information, refer to the “References and Recommended Reading” appendix in the *Cisco IOS Configuration Fundamentals and Network Management Command Reference*, Release 12.3 T.

Switch Priority

You can globally configure the priority of an individual switch when two switches tie for position as the root switch, or you can configure the likelihood that a switch will be selected as the root switch. This priority is determined by default; however, you can change it.

Interface Priority

You can change the priority for an interface. When two switches tie for position as the root switch, you configure an interface priority to break the tie. The switch with the lowest interface value is elected.

Path Cost Assignment

Each interface has a path cost associated with it. By convention, the path cost is 1000/data rate of the attached LAN, in Mbps.

BPDU Intervals Adjustment

You can adjust three different BPDU intervals. The interval between hello BPDUs can be set. The forward-delay interval is the amount of time spent listening for topology change information after an interface has been activated for switching and before forwarding actually begins. The maximum-idle interval specifies the amount of time the switch waits to hear BPDUs from the root switch. If a switch does not hear BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology.

Note Each switch in a spanning tree adopts the interval between hello BPDUs, the forward delay interval, and the maximum idle interval parameters of the root switch, regardless of what its individual configuration might be.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group* **hello-time** *seconds*
4. **bridge** *bridge-group* **forward-time** *seconds*
5. **bridge** *bridge-group* **max-age** *seconds*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`bridge`** *`bridge-group`* **`hello-time`** *`seconds`*
	Example:
	`Router(config)# bridge 10 hello-time 5`
		Specifies the interval between hello BPDUs.
		• Use the *bridge-group* argument to specify the bridge group number. The range is from 1 to 255.
		• Use the *seconds* argument to enter a number from 1 to 10. The default is 2 seconds.

Step 4	**`bridge`** *`bridge-group`* **`forward-time`** *`seconds`*
	Example:
	`Router(config)# bridge 10 forward-time 10`
		Specifies the forward-delay interval.
		• Use the *bridge-group* argument to specify the bridge group number. The range is from 1 to 255.
		• Use the *seconds* argument to enter a number from 10 to 200. The default is 20 seconds.

	Command or Action	Purpose

Step 5	**`bridge-group`** *`bridge-group`* **`max-age`** *`seconds`*
	Example:
	`Router(config)# bridge-group 10 max-age 30`
		Specifies the interval the switch waits to hear BPDUs from the root switch.
		• Use the *bridge-group* argument to specify the bridge group number. The range is from 1 to 255.
		• Use the *seconds* argument to enter a number from 10 to 200. The default is 30 seconds.

Step 6	**`exit`**
	Example:
	`Router(config)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Disabling the Spanning Tree on an Interface

Perform this task to disable spanning tree on an interface. When a loop-free path exists between any two switched subnetworks, you can prevent BPDUs generated in one switching subnetwork from impacting devices in the other switching subnetwork, yet still permit switching throughout the network as a whole. For example, when switched LAN subnetworks are separated by a WAN, BPDUs can be prevented from traveling across the WAN link.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **bridge** *bridge-group* **spanning-disabled**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port* **Example:** `Router(config)# interface gigabitethernet 0/1`	Selects the Ethernet interface on which the bridge group is assigned and enters interface configuration mode. The specified interface must be one of the following: • A routed port: a physical port that you have configured as a Layer 3 port by entering the **no switchport** interface configuration command. • An SVI: a VLAN interface that you created by using the **interface vlan** *vlan-id* global configuration command. • These ports must have IP addresses assigned to them.
Step 4	**bridge** *bridge-group* **spanning-disabled** **Example:** `Router(config-if)# bridge 10 spanning-disabled`	Disables spanning tree on the interface. • Use the *bridge-group* argument to specify the bridge group number. The range is from 1 to 255.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode. • Repeat this command to exit global configuration mode and return to privileged EXEC mode.

Configuring Network Security with ACLs at Layer 2

This section contains the following tasks:

- Configuring a Numbered Standard ACL, page 177
- Configuring a Numbered Extended ACL, page 179
- Configuring a Named Standard ACL, page 182
- Configuring a Named Extended ACL, page 184
- Applying the ACL to an Interface, page 185

Configuring ACLs on Layer 2 interfaces is the same as configuring ACLs on Cisco routers. The process is briefly described here. For more detailed information on configuring router ACLs, refer to the "Configuring IP Services" chapter in the *Cisco IP Configuration Guide.* For detailed information about the commands, refer to *Cisco IOS IP Command Reference* for Cisco IOS Release 12.3 T. For a list of Cisco IOS features not supported on the EtherSwitch network module, see the following section.

Restrictions

The EtherSwitch network module does not support these Cisco IOS router ACL-related features:

- Non-IP protocol ACLs (see Table 15 on page 176).
- Bridge-group ACLs.
- IP accounting.
- ACL support on the outbound direction.
- Inbound and outbound rate limiting (except with QoS ACLs).
- IP packets with a header length of less than five are not to be access-controlled.

- Reflexive ACLs.
- Dynamic ACLs.
- ICMP-based filtering.
- IGMP-based filtering.

Creating Standard and Extended IP ACLs

This section describes how to create switch IP ACLs. An ACL is a sequential collection of permit and deny conditions. The switch tests packets against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

An ACL must first be created by specifying an access list number or name and access conditions. The ACL can then be applied to interfaces or terminal lines.

The software supports these styles of ACLs or IP access lists:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

ACL Numbers

The number you use to denote your ACL shows the type of access list that you are creating. Table 15 lists the access list number and corresponding type and shows whether or not they are supported by the switch. The EtherSwitch network module supports IP standard and IP extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 15 Access List Numbers

ACL Number	Type	Supported
1–99	IP standard access list	Yes
100–199	IP extended access list	Yes
200–299	Protocol type-code access list	No
300–399	DECnet access list	No
400–499	XNS standard access list	No
500–599	XNS extended access list	No
600–699	AppleTalk access list	No
700–799	48-bit MAC address access list	No
800–899	IPX standard access list	No
900–999	IPX extended access list	No
1000–1099	IPX SAP access list	No
1100–1199	Extended 48-bit MAC address access list	No
1200–1299	IPX summary address access list	No

Table 15 Access List Numbers (continued)

ACL Number	Type	Supported
1300–1999	IP standard access list (expanded range)	Yes
2000–2699	IP extended access list (expanded range)	Yes

Note In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Note An attempt to apply an unsupported ACL feature to an EtherSwitch network module interface produces an error message.

Including Comments About Entries in ACLs

You can use the **remark** command to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

For IP numbered standard or extended ACLs, use the **access-list** *access-list number* **remark** *remark* global configuration command to include a comment about an access list. To remove the remark, use the **no** form of this command.

For an entry in a named IP ACL, use the **remark** *access-list* global configuration command. To remove the remark, use the **no** form of this command.

Configuring a Numbered Standard ACL

Perform this task to create a numbered standard ACL.

Note When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the ask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit** | **remark**} {*source source-wildcard* | **host** *source* | **any**}

4. **exit**
5. **show access-lists** [*number* | *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**access-list** *access-list-number* {**deny** | **permit** | **remark**} {*source source-wildcard* | **host** *source* | **any**}
	Example:
	`Router(config)# access-list 2 deny host 172.17.198.102`
		Defines a standard IP ACL by using a source address and wildcard.
		• The *access-list-number* is a decimal number from 1 to 99 or 1300 to 1999.
		• Enter the **deny** or **permit** keywords to specify whether to deny or permit access if conditions are matched.
		• The *source* is the source address of the network or host from which the packet is being sent, and is a 32-bit number in dotted-decimal format.
		• The *source-wildcard* applies wildcard bits to the source address.
		• The keyword **host** as an abbreviation for source and source-wildcard of *source* 0.0.0.0.
		• The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 5	**show access-lists** [*number* | *name*] **Example:** `Router# show access-lists`	Displays access list configuration information.

Configuring a Numbered Extended ACL

Perform this task to create a numbered extended ACL.

Extended ACLs

Although standard ACLs use only source addresses for matching, you can use an extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. Some protocols also have specific parameters and keywords that apply to that protocol.

These IP protocols are supported (protocol keywords are in parentheses in bold): Internet Protocol (**ip**), Transmission Control Protocol (**tcp**), or User Datagram Protocol (**udp**).

Supported parameters can be grouped into these categories:

- TCP
- UDP

Table 16 lists the possible filtering parameters for ACEs for each protocol type.

Table 16 Filtering Parameter ACEs Supported by Different IP Protocols

Filtering Parameter	TCP	UDP
Layer 3 Parameters:		
IP ToS byte[1]	No	No
Differentiated Services Code Point (DSCP)	No	No
IP source address	Yes	Yes
IP destination address	Yes	Yes
Fragments	No	No
TCP or UDP	Yes	Yes
Layer 4 Parameters		
Source port operator	Yes	Yes
Source port	Yes	Yes
Destination port operator	Yes	Yes
Destination port	Yes	Yes
TCP flag	No	No

[1] No support for type of service (TOS) minimize monetary cost bit.

For more details on the specific keywords relative to each protocol, refer to the *Cisco IP Command Reference* for Cisco IOS Release 12.3 T.

Note The EtherSwitch network module does not support dynamic or reflexive access lists. It also does not support filtering based on the minimize-monetary-cost type of service (TOS) bit.

When creating ACEs in numbered extended access lists, remember that after you create the list, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

Use the **no access-list** *access-list-number* global configuration command to delete the entire access list. You cannot delete individual ACEs from numbered access lists.

After an ACL is created, any additions (possibly entered from the terminal) are placed at the end of the list. You can add ACEs to an ACL, but deleting any ACE deletes the entire ACL.

Note When creating an ACL, remember that, by default, the end of the access list contains an implicit deny statement for all packets if it did not find a match before reaching the end.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*]
4. **exit**
5. **show access-lists** [*number* | *name*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**access-list** *access-list-number* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*] **Example:** `Router(config)# access-list 102 deny tcp 172.17.69.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet`	Defines an extended IP access list and the access conditions. • The *access-list-number* is a decimal number from 100 to 199 or 2000 to 2699. • Enter the **deny** or **permit** keywords to specify whether to deny or permit access if conditions are matched. • For *protocol*, enter the name or number of an IP protocol: **ip**, **tcp**, or **udp**. To match any Internet protocol (including TCP and UDP), use the keyword **ip**. • The *source* is the source address of the network or host from which the packet is being sent, and is a 32-bit number in dotted-decimal format. • The *source-wildcard* applies wildcard bits to the source address. • The keyword **host** as an abbreviation for source and source-wildcard of *source* 0.0.0.0. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The *operator* defines a destination or source port and can be only **eq** (equal). • If operator is after *source source-wildcard*, conditions match when the source port matches the defined port. • If operator is after *destination destination-wildcard*, conditions match when the destination port matches the defined port. • The *port* is a decimal number or name of a TCP or UDP port. The number can be from 0 to 65535. • Use TCP port names only for TCP traffic. • Use UDP port names only for UDP traffic. **Note** Only the **ip**, **tcp**, and **udp** protocols are supported on Ethernet switch interfaces. • The *destination* is the address of the network or host to which the packet is being sent, and is a 32-bit number in dotted-decimal format. • The *destination-wildcard* applies wildcard bits to the destination address. • The keyword **host** as an abbreviation for *destination* and *destination-wildcard* of *destination* 0.0.0.0. • The keyword **any** as an abbreviation for *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.

	Command or Action	Purpose

Step 4	`exit`
	Example:
	`Router(config)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Step 5	**`show access-lists`** [*`number`* | *`name`*] **Example:** `Router# show access-lists`	Displays access list configuration information.

What to Do Next

After creating an ACL, you must apply it to an interface, as described in the "Applying the ACL to an Interface" section on page 185.

Configuring a Named Standard ACL

Perform this task to create a named standard ACL.

Named Standard ACL Creation

You can identify IP ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IP access lists on a switch than if you use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, not all commands that use IP access lists accept a named ACL.

Note The name you give to a standard ACL or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines and limitations before configuring named ACLs:

- A standard ACL and an extended ACL cannot have the same name.
- Numbered ACLs are also available, as described in the "Creating Standard and Extended IP ACLs" section on page 176.

Note When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the ask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list standard** {*access-list-number* | *name*}

4. **deny** {*source source-wildcard* | **host** *source* | **any**}
   or
   permit {*source source-wildcard* | **host** *source* | **any**}
5. **exit**
6. **show access-lists** [*number* | *name*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ip access-list standard`** {*`access-list-number`* | *`name`*}
	Example:
	`Router(config)# ip access-list standard sales`
		Defines a standard IP access list using a name and enters access-list configuration mode.
		- The *name* argument can be a decimal number from 1 to 99.

Step 4	**`deny`** {*`source source-wildcard`* | **`host`** *`source`* | **`any`**}
	or
	`permit` {*`source source-wildcard`* | **`host`** *`source`* | **`any`**}
	Example:
	`Router(config-acl# deny 10.2.1.3 any`
	Example:
	`Router(config-acl)# permit 10.2.1.4 any`
		Specifies one or more conditions denied or permitted to determine if the packet is forwarded or dropped.
		- **host** *source* represents a source and source wildcard of *source* 0.0.0.0.
		- **any** represents a source and source wildcard of 0.0.0.0 255.255.255.255.

Step 5	**`exit`**
	Example:
	`Router(config)# exit`
		Exits access-list configuration mode and returns the router to global configuration mode.
		- Repeat this command to exit global configuration mode and return to privileged EXEC mode.

Step 6	**`show access-lists`** [*`number`* | *`name`*] **Example:** `Router# show access-lists sales`	Displays access list configuration information.

Configuring a Named Extended ACL

You can identify IP ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IP access lists on a switch than if you use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, not all commands that use IP access lists accept a named ACL.

Note The name you give to a standard ACL or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines and limitations before configuring named ACLs:

- A standard ACL and an extended ACL cannot have the same name.
- Numbered ACLs are also available, as described in the "Creating Standard and Extended IP ACLs" section on page 176.

Note When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the ask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** {*access-list-number* | *name*}
4. **deny** *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*]
   or
   permit {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*]
5. **exit**
6. **show access-lists** [*number* | *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**ip access-list extended** {*access-list-number* | *name*}
	Example:
	`Router(config)# ip access-list extended marketing`
		Defines an extended IP access list using a name and enters access-list configuration mode.
		• The *name* argument can be a decimal number from 100 to 199.

Step 4	**deny** {*source source-wildcard* | **host** *source* | **any**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*]
	or
	permit {*source source-wildcard* | **host** *source* | **any**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*]
	Example:
	`Router(config-acl# deny tcp any any`
	or
	`Router(config-acl)# permit tcp 10.2.1.4 0.0.0.255 eq telnet`
		Specifies one or more conditions denied or permitted to determine if the packet is forwarded or dropped.
		See the "Configuring a Numbered Extended ACL" section on page 179 for definitions of protocols and other keywords.
		• **host** *source* represents a source and source wildcard of *source* 0.0.0.0, and **host** *destination* represents a destination and destination wildcard of *destination* 0.0.0.0.
		• **any** represents a source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.

Step 5	**exit** **Example:** `Router(config-acl)# exit`	Exits access-list configuration mode and returns the router to global configuration mode. • Repeat this command to exit global configuration mode and return to privileged EXEC mode.
Step 6	**show access-lists** [*number* | *name*] **Example:** `Router# show access-lists marketing`	Displays access list configuration information.

Applying the ACL to an Interface

Perform this task to control access to a Layer 2 or Layer 3 interface. After you create an ACL, you can apply it to one or more interfaces. ACLs can be applied on inbound interfaces. This section describes how to accomplish this task for network interfaces. Note these guidelines:

- When controlling access to a line, you must use a number. Numbered ACLs can be applied to lines.
- When controlling access to an interface, you can use a name or number.

Note The **ip access-group** interface configuration command is only valid when applied to a Layer 2 interface or a Layer 3 interface. If applied to a Layer 3 interface, the interface must have been configured with an IP address. ACLs cannot be applied to interface port-channels.

For inbound ACLs, after receiving a packet, the switch checks the packet against the ACL. If the ACL permits the packet, the switch continues to process the packet. If the ACL rejects the packet, the switch discards the packet.

When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied to the interface and permits all packets. Remember this behavior if you use undefined ACLs for network security.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **ip access-group** {*access-list-number* | *name*} **in**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface {ethernet | fastethernet | gigabitethernet} slot/port`
	Example:
	`Router(config)# interface gigabitethernet 0/3`
		Specifies the Ethernet interface to which the ACL will be applied and enters interface configuration mode.
		• The interface must be a Layer 2 interface or a routed port.

	Command or Action	Purpose
Step 4	**ip access-group** {*access-list-number* | *name*} **in** **Example:** `Router(config)# ip access-group sales in`	Controls access to the specified interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this step one more time to exit global configuration mode.

Configuring Quality of Service (QoS) on the EtherSwitch network module

This section consists of the following tasks that must be performed to configure QoS on your EtherSwitch network module:

- Configuring Classification Using Port Trust States, page 189
- Configuring a QoS Policy, page 191

Prerequisites

Before configuring QoS, you must have a thorough understanding of the following items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

Restrictions

- If you have EtherChannel ports configured on your switch, you must configure QoS classification, policing, mapping, and queueing on the individual physical ports that comprise the EtherChannel. You must decide whether the QoS configuration should match on all ports in the EtherChannel.
- It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are transmitted as best-effort. IP fragments are denoted by fields in the IP header.
- Control traffic (such as spanning-tree Bridge Protocol Data Units (BPDUs) and routing update packets) received by the switch are subject to all ingress QoS processing.
- Only one ACL per class map and only one **match** command per class map are supported. The ACL can have multiple access control entries, which are commands that match fields against the contents of the packet.
- Policy maps with ACL classification in the egress direction are not supported and cannot be attached to an interface by using the **service-policy input** *policy-map-name* interface configuration command.
- In a policy map, the class named class-default is not supported. The switch does not filter traffic based on the policy map defined by the **class class-default** policy-map configuration command.

For more information on guidelines for configuring ACLs, see the "Classification Based on QoS ACLs" section on page 112.

QoS on Switching Devices

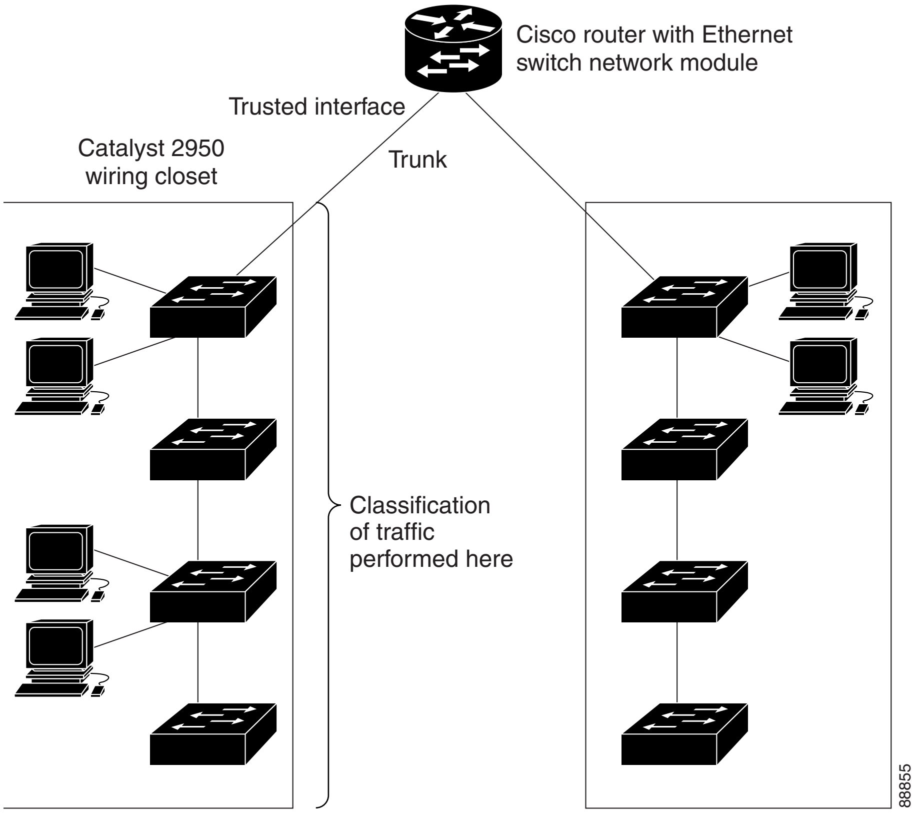
Default Settings

- The default port CoS value is 0.
- The default port trust state is untrusted.
- No policy maps are configured.
- No policers are configured.
- The default CoS-to-DSCP map is shown in Table 17 on page 196.
- The default DSCP-to-CoS map is shown in Table 18 on page 197.

Trust State on Ports and SVIs Within the QoS Domain

Packets entering a QoS domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the QoS domain. Figure 23 shows a sample network topology.

Figure 23 Port Trusted States within the QoS Domain


Cisco router with Ethernet switch network module
Trusted interface
Catalyst 2950 wiring closet
Trunk
Classification of traffic performed here
88855

Configuring Classification Using Port Trust States

Perform this task to configure the port to trust the classification of the traffic that it receives, and then define the default CoS value of a port or to assign the default Cos to all incoming packets on the port.

Note The **mls qos cos** command replaced the **switchport priority** command in Cisco IOS Release 12.1(6)EA2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
4. **mls qos trust** {**cos** | **dscp**}
5. **mls qos cos** {*default-cos* | **override**}
6. **exit**
7. **show mls qos interface** [*interface-type slot*/*port*] [**policers**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface`** {**`ethernet`** | **`fastethernet`** | **`gigabitethernet`**} *`slot`*/*`port`*
	Example:
	`Router(config)# interface fastethernet 0/1`
		Selects the Ethernet interface to be trusted and enters interface configuration mode.
		• Valid interfaces include physical interfaces and SVIs.

	Command or Action	Purpose

Step 4	**mls qos trust** {**cos** | **dscp**}
	Example:
	`Router(config-if)# mls qos trust cos`
		Configures the port trust state.
		• By default, the port is not trusted.
		• Use the **cos** keyword setting if your network is composed of Ethernet LANs, Catalyst 2950 switches, and has no more than two types of traffic.
		• Use the **cos** keyword if you want ingress packets to be classified with the packet CoS values. For tagged IP packets, the DSCP value of the packet is modified based on the CoS-to-DSCP map. The egress queue assigned to the packet is based on the packet CoS value.
		• Use the **dscp** keyword if your network is not composed of only Ethernet LANs and if you are familiar with sophisticated QoS features and implementations.
		• Use the **dscp** keyword if you want ingress packets to be classified with packet DSCP values. For non-IP packets, the packet CoS value is used for tagged packets; the default port CoS is used for untagged packets. Internally, the switch modifies the CoS value by using the DSCP-to-CoS map.
		• Use the **dscp** keyword if you are using an SVI that is a VLAN interface that you created by using the **interface vlan** *vlan-id* global configuration command. The DCSP-to-CoS map will be applied to packets arriving from a router to the EtherSwitch network module through an SVI.

Step 5	**mls qos cos** {*default-cos* | **override**}
	Example:
	`Router(config-if)# mls qos cos 5`
		Configures the default CoS value for the port.
		• Use the *default-cos* argument to specify a default CoS value to be assigned to a port. If the port is CoS trusted and packets are untagged, the default CoS value becomes the CoS value for the packet. The CoS range is 0 to 7. The default is 0.
		• Use the **override** keyword to override the previously configured trust state of the incoming packets and to apply the default port CoS value to all incoming packets. By default, CoS override is disabled.
		• Use the **override** keyword when all incoming packets on certain ports deserve higher priority than packets entering from other ports. Even if a port was previously set to trust DSCP, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with this command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns the router to global configuration mode. • Repeat this step one more time to exit global configuration mode.
Step 7	**show mls qos interface** [*interface-type slot***/***port*] [**policers**] **Example:** `Router# show mls qos interface fastethernet 0/1`	(Optional) Displays information about Fast Ethernet interfaces.

Examples

The following is sample output from the **show mls qos interface fastethernet0/1** command:

```
Router# show mls qos interface fastethernet 0/1

FastEthernet0/1
trust state: trust cos
COS override: dis
default COS: 0
```

Configuring a QoS Policy

This section contains the following tasks:

- Classifying Traffic by Using ACLs, page 191
- Classifying Traffic Using Class Maps, page 191
- Classifying, Policing, and Marking Traffic Using Policy Maps, page 193

Configuring a QoS policy typically requires classifying traffic into classes, configuring policies applied to those traffic classes, and attaching policies to interfaces.

For background information, see the "Classification" section on page 112 and the "Policing and Marking" section on page 113.

Classifying Traffic by Using ACLs

You can classify IP traffic by using IP standard or IP extended ACLs. To create an IP standard ACL for IP traffic, refer to the "Configuring a Numbered Standard ACL" section on page 177 and to create an IP extended ACL for IP traffic refer to the "Configuring a Numbered Extended ACL" section on page 179.

Classifying Traffic Using Class Maps

Perform this task to create a class map and to define the match criteria for classifying traffic. You use the **class-map** global configuration command to isolate a specific traffic flow (or class) from all other traffic and to name it. The class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as an ACL. The match criterion is defined with one match statement entered within the class-map configuration mode.

Note You can also create class maps during policy map creation by using the **class** policy-map configuration command. For more information, see the "Classifying, Policing, and Marking Traffic Using Policy Maps" section on page 193.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit** | **remark**} {*source source-wildcard* | **host** *source* | **any**}
   or
   access-list *access-list-number* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator-port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator-port*]
4. **class-map** *class-map-name*
5. **match access-group** *acl-index-or-name*
6. **exit**
7. **show class-map** [*class-map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit** | **remark**} {*source source-wildcard* | **host** *source* | **any**} or **access-list** *access-list-number* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*] **Example:** `Router(config)# access-list 103 permit any any tcp eq 80`	Creates an IP standard or extended ACL for IP traffic. • Repeat this command as many times as necessary. • For more information, see the "Configuring a Numbered Standard ACL" section on page 177 and the "Configuring a Numbered Extended ACL" section on page 179. • Deny statements are not supported for QoS ACLS. See the "Classification Based on QoS ACLs" section on page 112 for more details.

	Command or Action	Purpose

Step 4	**`class-map`** *`class-map-name`*
	Example:
	`Router(config)# class-map class1`
		Creates a class map, and enters class-map configuration mode.
		• By default, no class maps are defined.
		• Use the *class-map-name* argument to specify the name of the class map.

Step 5	**`match access-group`** *`acl-index-or-name`*
	Example:
	`Router(config-cmap)# match access-group 103`
		Defines the match criteria to classify traffic.
		• By default, no match criteria is supported.
		• Only one match criteria per class map is supported, and only one ACL per class map is supported.
		• Use the *acl-index-or-name* argument to specify the number or name of the ACL created in Step 3.

Step 6	**`exit`**
	Example:
	`Router(config-cmap)# exit`
		Exits class map configuration mode and returns the router to global configuration mode.
		• Repeat this step one more time to exit global configuration mode.

Step 7	**`show class-map`** `[`*`class-map-name`*`]`
	Example:
	`Router# show class-map class1`
		(Optional) Displays class maps and their matching criteria.

Classifying, Policing, and Marking Traffic Using Policy Maps

Perform this task to create a policy map. A policy map specifies which traffic class to act on. Actions can include trusting the CoS or DSCP values in the traffic class; setting a specific DSCP value in the traffic class; and specifying the traffic bandwidth limitations for each matched traffic class (policer) and the action to take when the traffic is out of profile (marking).

A separate policy-map class can exist for each type of traffic received through an interface. You can attach only one policy map per interface in the input direction.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit** | **remark**} {*source source-wildcard* | **host** *source* | **any**}
   or
   access-list *access-list-number* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator-port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator-port*]
4. **policy-map** *policy-map-name*
5. **class** *class-map-name* [**access-group** *acl-index-or-name*]
6. **police** {*bps* | **cir** *bps*} [*burst-byte* | **bc** *burst-byte*] **conform-action transmit** [**exceed-action** {**drop** | **dscp** *dscp-value*}]
7. **exit**

8. **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot*/*port*
9. **service-policy input** *policy-map-name*
10. **exit**
11. **show policy-map** *policy-map-name* **class** *class-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit** | **remark**} {*source source-wildcard* | **host** *source* | **any**} or **access-list** *access-list-number* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*] **Example:** `Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255`	Creates an IP standard or extended ACL for IP traffic. • Repeat this command as many times as necessary. • For more information, see the "Configuring a Numbered Standard ACL" section on page 177 and the "Configuring a Numbered Extended ACL" section on page 179. **Note** Deny statements are not supported for QoS ACLS. See the "Classification Based on QoS ACLs" section on page 112 for more details.
Step 4	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map flow1t`	Creates a policy map by entering the policy map name, and enters policy-map configuration mode. • By default, no policy maps are defined. • The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.

	Command or Action	Purpose

Step 5	**class** {*class-map-name* | **class-default**} [**access-group** *acl-index-or-name*]
	Example:
	`Router(config-pmap)# class ipclass1`
		Defines a traffic classification, and enters policy-map class configuration mode.
		• By default, no policy map class maps are defined.
		• If a traffic class has already been defined by using the **class-map** global configuration command, specify its name for *class-map-name* in this command.
		• For **access-group** *acl-index-or-name*, specify the number or name of the ACL created in Step 3.
		• In a policy map for the EtherSwitch network module, the class named **class-default** is not supported. The switch does not filter traffic based on the policy map defined by the **class class-default** policy-map configuration command.

Step 6	**police** {*bps* | **cir** *bps*} [*burst-byte* | **bc** *burst-byte*] **conform-action transmit** [**exceed-action** {**drop** | **dscp** *dscp-value*}] **Example:** `Router(config-pmap)# police 5000000 8192 conform-action transmit exceed-action dscp 10`	Defines a policer for the classified traffic. • You can configure up to 60 policers on ingress Gigabit-capable Ethernet ports and up to 6 policers on ingress 10/100 Ethernet ports. • For *bps*, specify average traffic rate or committed information rate in bits per second (bps). The range is 1 Mbps to 100 Mbps for 10/100 Ethernet ports and 8 Mbps to 1000 Mbps for the Gigabit-capable Ethernet ports. • For *burst-byte*, specify the normal burst size or burst count in bytes. • (Optional) Specify the action to take when the rates are exceeded. Use the **exceed-action drop** keywords to drop the packet. Use the **exceed-action dscp** *dscp-value* keywords to mark down the DSCP value and transmit the packet.
Step 7	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy map configuration mode and returns the router to global configuration mode.
Step 8	**interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot***/***port* **Example:** `Router(config)# interface fastethernet 5/6`	Enters interface configuration mode, and specifies the interface to attach to the policy map. • Valid interfaces include physical interfaces.
Step 9	**service-policy input** *policy-map-name* **Example:** `Router(config-if)# service-policy input flow1t`	Applies a policy map to the input of a particular interface. • Only one policy map per interface per direction is supported. • Use **input** *policy-map-name* to apply the specified policy map to the input of an interface.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Router(config-class-map)# exit`	Exits class map configuration mode and returns the router to global configuration mode. • Repeat this step one more time to exit global configuration mode.
Step 11	**show policy-map** *policy-map-name* **class** *class-map-name* **Example:** `Router# show policy-map flow1t class class1`	(Optional) Displays the configuration for the specified class of the specified policy map.

Configuring the CoS-to-DSCP Map

Perform this task to modify the CoS-to-DSCP map. You use the CoS-to-DSCP map to map CoS values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic.

Table 17 shows the default CoS-to-DSCP map.

Table 17 Default CoS-to-DSCP Map

CoS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	26	32	46	48	56

If these values are not appropriate for your network, you need to modify them. These CoS-to-DSCP mapping numbers follow the numbers used in deploying Cisco AVVID and may be different from the mapping numbers used by the EtherSwitch network module, Cisco Catalyst 2950, Cisco Catalyst 3550, and other switches.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mls qos map cos-dscp** *dscp1...dscp8*
4. **exit**
5. **show mls qos maps cos-dscp**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`mls qos map cos-dscp`** *`dscp1...dscp8`*
	Example:
	`Router(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56`
		Modifies the CoS-to-DSCP map.
		• For *dscp1...dscp8*, enter eight DSCP values that correspond to CoS values 0 to 7. Separate each DSCP value with a space.
		• The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

Step 4	**`exit`**
	Example:
	`Router(config)# exit`
		Exits global configuration mode and returns the router to privileged EXEC mode.

Step 5	**`show mls qos maps cos-dscp`**
	Example:
	`Router# show mls qos maps cos-dscp`
		(Optional) Displays the CoS-to-DSCP map.

Configuring the DSCP-to-CoS Map

Perform this task to modify the DSCP-to-CoS map. You use the DSCP-to-CoS map to map DSCP values in incoming packets to a CoS value, which is used to select one of the four egress queues. The EtherSwitch network modules support these DSCP values: 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

Table 18 shows the default DSCP-to-CoS map.

Table 18 Default DSCP-to-CoS Map

DSCP values	0	8, 10	16, 18	24, 26	32, 34	40, 46	48	56
CoS values	0	1	2	3	4	5	6	7

If these values are not appropriate for your network, you need to modify them. These DSCP-to-CoS mapping numbers follow the numbers used in deploying Cisco AVVID and may be different from the mapping numbers used by the EtherSwitch network module, Cisco Catalyst 2950, Cisco Catalyst 3550, and other switches.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mls qos map dscp-cos** *dscp-list* **to** *cos*
4. **exit**
5. **show mls qos maps dscp-to-cos**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mls qos map dscp-cos** *dscp-list* **to** *cos* *Example:* `Router(config)# mls qos map dscp-cos 26 48 to 7`	Modifies the DSCP-to-CoS map. • For *dscp-list*, enter up to 13 DSCP values separated by spaces. Then enter the **to** keyword. • For *cos*, enter the CoS value to which the DSCP values correspond. • The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56. The CoS range is 0 to 7.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.
Step 5	**show mls qos maps dscp-to-cos** **Example:** `Router# show mls qos maps dscp-to-cos`	(Optional) Displays the DSCP-to-CoS map.

Configuration Examples for the EtherSwitch Network Module

This section contains the following configuration examples:

- Configuring VLANs: Example, page 199
- Configuring VTP: Example, page 199
- Configuring Spanning Tree: Examples, page 200
- Configuring Layer 2 Interfaces: Examples, page 201

Configuring VLANs: Example

The following example shows how to configure a VLAN:

```
Router# vlan database
Router(vlan)# vlan 2 media ethernet name vlan1502
VLAN 2 added:
Name: VLAN1502
Router(vlan)# exit
APPLY completed.
Exiting....
```

Configuring VTP: Example

The following example shows how to configure a VTP server, configure a VTP client, configure VTP version 2, and disable VTP mode on the router:

```
Router# vlan database
Router(vlan)# vtp server
Setting device to VTP SERVER mode.
Router(vlan)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Router(vlan)# vtp password WATER
Setting device VLAN database password to WATER.
Router(vlan)# vtp client
Setting device to VTP CLIENT mode.
Router(vlan)# vtp v2-mode
V2 mode enabled.
Router(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
Router(vlan)# exit
APPLY completed.
Exiting....
```

Configuring Spanning Tree: Examples

The following example shows spanning tree being enabled on VLAN 200 and the bridge priority set to 33792. The hello time for VLAN 200 is set at 7 seconds, the forward delay time set at 21 seconds, and the maximum aging time at 36 seconds. BackboneFast is enable, the VLAN port priority of an interface is configured to be 64 and the spanning tree port cost of the Fast Ethernet interface 5/8 is set at 18.

```
Router# configure terminal
Router(config)# spanning-tree vlan 200
Router(config)# spanning-tree vlan 200 priority 33792
Router(config)# spanning-tree vlan 200 hello-time 7
Router(config)# spanning-tree vlan 200 forward-time 21
Router(config)# spanning-tree vlan 200 max-age 36
Router(config)# spanning-tree backbonefast
Router(config-if)# exit
Router(config)# interface fastethernet 5/8
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# spanning-tree cost 18
Router(config-if)# exit
Router(config)# exit
```

The following example shows how to verify the configuration of VLAN 200 on the interface when it is configured as a trunk port:

```
Router# show spanning-tree vlan 200

Port 264 (FastEthernet5/8) of VLAN200 is forwarding
Port path cost 19, Port priority 64, Port Identifier 129.8.
   Designated root has priority 32768, address 0010.0d40.34c7
   Designated bridge has priority 32768, address 0010.0d40.34c7
   Designated port id is 128.1, designated path cost 0
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 0, received 13513
```

The following example shows how to verify the configuration of the interface when it is configured as an access port:

```
Router# show spanning-tree interface fastethernet 5/8

 Port 264 (FastEthernet5/8) of VLAN200 is forwarding
   Port path cost 18, Port priority 100, Port Identifier 129.8.
   Designated root has priority 32768, address 0010.0d40.34c7
   Designated bridge has priority 32768, address 0010.0d40.34c7
   Designated port id is 128.1, designated path cost 0
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 0, received 13513
```

The following example shows spanning tree being enabled on VLAN 150:

```
Router# configure terminal
Router(config)# spanning-tree vlan 150
Router(config)# end
Router#
```

Note Because spanning tree is enabled by default, issuing a **show running-config** command to view the resulting configuration will not display the command you entered to enable spanning tree.

The following example shows spanning tree being disabled on VLAN 200:

```
Router# configure terminal
Router(config)# no spanning-tree vlan 200
Router(config)# end
```

The following example shows the switch device being configured as the root bridge for VLAN 10, with a network diameter of 4:

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

Configuring Layer 2 Interfaces: Examples

This section contains the following examples:

- Single Range Configuration: Example, page 201
- Multiple Range Configuration: Example, page 201
- Range Macro Definition: Example, page 202
- Optional Interface Features: Example, page 202
- Configuring an Ethernet Interface as a Layer 2 Trunk: Example, page 202

Single Range Configuration: Example

The following example shows all Fast Ethernet interfaces 5/1 to 5/5 being reenabled:

```
Router(config)# interface range fastethernet 5/1 - 5
Router(config-if)# no shutdown
Router(config-if)#
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/5, changed
state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/3, changed
state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/4, changed
state to up
Router(config-if)#
```

Multiple Range Configuration: Example

The following example shows how to use a comma to add different interface type strings to the range to reenable all Fast Ethernet interfaces in the range 5/1 to 5/5 and both Gigabit Ethernet interfaces 1/1 and 1/2:

```
Router(config-if)# interface range fastethernet 5/1 - 5, gigabitethernet 1/1 - 2
Router(config-if)# no shutdown
Router(config-if)#
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
```

```
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/2, changed state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/5, changed
state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/3, changed
state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/4, changed
state to up
Router(config-if)#
```

Range Macro Definition: Example

The following example shows an interface-range macro named enet_list being defined to select Fast Ethernet interfaces 5/1 through 5/4:

```
Router(config)# define interface-range enet_list fastethernet 5/1 - 4

Router(config)#
```

The following example shows how to change to the interface-range configuration mode using the interface-range macro enet_list:

```
Router(config)# interface range macro enet_list

Router(config-if)#
```

Optional Interface Features: Example

The following example shows the interface speed being set to 100 Mbps on the Fast Ethernet interface 5/4, the interface duplex mode set to full, and a description being added for the interface:

```
Router(config)# interface fastethernet 5/4
Router(config-if)# speed 100
Router(config-if)# duplex full
Router(config-if)# description Channel-group to "Marketing"
```

Configuring an Ethernet Interface as a Layer 2 Trunk: Example

The following example shows how to configure the Fast Ethernet interface 5/8 as an 802.1Q trunk. This example assumes that the neighbor interface is configured to support 802.1Q trunking:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/8
Router(config-if)# shutdown
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# no shutdown
Router(config-if)# end
Router# exit
```

Configuring Voice and Data VLANs: Examples

This section contains the following examples:

- Separate Voice and Data VLANs: Example, page 203
- Inter-VLAN Routing: Example, page 203

- Single Subnet Configuration: Example, page 204
- Ethernet Ports on IP Phones with Multiple Ports: Example, page 204

Separate Voice and Data VLANs: Example

The following example shows separate VLANs being configured for voice and data on the EtherSwitch network module:

```
interface fastethernet5/1
 description DOT1Q port to IP Phone
 switchport native vlan 50
 switchport mode trunk
 switchport voice vlan 150

interface vlan 150
 description voice vlan
 ip address 10.150.1.1 255.255.255.0
 ip helper-address 172.20.73.14 (See Note below)

interface vlan 50
 description data vlan
 ip address 10.50.1.1 255.255.255.0
```

This configuration instructs the IP phone to generate a packet with an 802.1Q VLAN ID of 150 with an 802.1p value of 5 (default for voice bearer traffic).

Note In a centralized CallManager deployment model, the DHCP server might be located across the WAN link. If so, an **ip helper-address** command pointing to the DHCP server should be included on the voice VLAN interface for the IP phone. This is done to obtain its IP address as well as the address of the TFTP server required for its configuration.

Cisco IOS supports a DHCP server function. If this function is used, the EtherSwitch network module serves as a local DHCP server and a helper address would not be required.

Inter-VLAN Routing: Example

Configuring inter-VLAN routing is identical to the configuration on an EtherSwitch network module with an MSFC. Configuring an interface for WAN routing is consistent with other Cisco IOS platforms.

The following example provides a sample configuration:

```
interface vlan 160
 description voice vlan
 ip address 10.6.1.1 255.255.255.0

interface vlan 60
 description data vlan
 ip address 10.60.1.1 255.255.255.0

interface serial1/0
 ip address 160.3.1.2 255.255.255.0
```

Note Standard IGP routing protocols such as RIP, IGRP, EIGRP, and OSPF are supported on the EtherSwitch network module. Multicast routing is also supported for PIM dense mode, sparse mode, and sparse-dense mode.

Single Subnet Configuration: Example

The EtherSwitch network module supports the use of an 802.1p-only option when configuring the voice VLAN. Using this option allows the IP phone to tag VoIP packets with a CoS of 5 on the native VLAN, while all PC data traffic is sent untagged.

The following example shows a single subnet configuration for the EtherSwitch network module switch:

```
interface fastethernet 5/2
 description Port to IP Phone in single subnet
 switchport access vlan 40
 switchport voice vlan dot1p
 spanning-tree portfast
```

The EtherSwitch network module instructs the IP phone to generate an 802.1Q frame with a null VLAN ID value but with an 802.1p value (default is COS of 5 for bearer traffic). The voice and data VLANs are both 40 in this example.

Ethernet Ports on IP Phones with Multiple Ports: Example

The following example illustrates the configuration on the IP phone:

```
interface fastethernet 2/2
 switchport voice vlan 5
 switchport mode trunk
```

The following example illustrates the configuration on the PC:

```
interface fastethernet 2/3
 switchport access vlan 10
```

Note Using a separate VLAN, and possibly a separate IP address space, may not be an option for some small branch offices due to the IP routing configuration. If the IP routing can handle an additional VLAN at the remote branch, you can use Cisco Network Registrar and secondary addressing.

Configuring 802.1x Authentication: Examples

This section contains the following examples:

- Enabling 802.1x Authentication: Example, page 205
- Configuring the Switch-to-RADIUS-Server Communication: Example, page 205
- Configuring 802.1x Parameters: Example, page 205

Enabling 802.1x Authentication: Example

The following example shows how to enable AAA and 802.1x on Fast Ethernet port 0/1:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# end
```

Configuring the Switch-to-RADIUS-Server Communication: Example

The following example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to rad123, matching the key on the RADIUS server:

```
Router(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

Configuring 802.1x Parameters: Example

The following example shows how to enable periodic reauthentication, set the number of seconds between reauthentication attempts to 4000, and set the quiet time to 30 seconds on the EtherSwitch network module. The number of seconds to wait for an EAP-request/identity frame before transmitting is set to 60 seconds and the number of times the switch device will send the EAP-request/identity frames before restarting the authentication process is set to 5. 802.1x is enabled on Fast Ethernet interface 0/1 and multiple hosts are permitted.

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
Router(config)# dot1x timeout quiet-period 30
Router(config)# dot1x timeout tx-period 60
Router(config)# dot1x max-req 5
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

Configuring Storm-Control: Example

The following example shows global multicast suppression being enabled at 70 percent on Gigabit Ethernet interface 1 and the configuration being verified:

```
Router# configure terminal
Router(config)# interface gigabitethernet0/2
Router(config-if)# storm-control multicast level 70
Router(config-if)# end
Router# show storm-control

Name: Gi0/2
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

```
Port Protected: Off
Unknown Unicast Traffic: Allowed
Unknown Multicast Traffic: Not Allowed

Broadcast Suppression Level: 100
Multicast Suppression Level: 70
Unicast Suppression Level: 100
```

Configuring Layer 2 EtherChannels: Example

- Layer 2 EtherChannels: Example, page 206
- Removing an EtherChannel: Example, page 206

Layer 2 EtherChannels: Example

The following example shows Fast Ethernet interfaces 5/6 and 5/7 being configured into port-channel 2 and forces the port to channel without Port Aggregation Protocol (PAgP). The EtherChannel is configured to use source and destination IP addresses.

```
Router# configure terminal
Router(config)# interface range fastethernet 5/6 - 7
Router(config-if)# channel-group 2 mode on
Router(config-if)# exit
Router(config)# port-channel load-balance src-dst-ip
```

Removing an EtherChannel: Example

The following example shows port-channel 1 being removed:

```
Router# configure terminal
Router(config)# no interface port-channel 1
Router(config)# end
```

Note Removing the port-channel also removes the channel-group command from the interfaces belonging to it.

Configuring Flow Control on Gigabit Ethernet Ports: Example

The following examples show how to turn transmit and receive flow control on and how to verify the flow-control configuration.

Port 4/0 flow control send administration status is set to on (port will send flowcontrol to far end):

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet4/0
Router(config-if)# flowcontrol send on
Router(config-if)# end
```

Port 4/0 flow control receive administration status is set to on (port will require far end to send flowcontrol):

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet4/0
Router(config-if)# flowcontrol receive on
Router(config-if)# end
```

The following example shows flow control configuration being verified:

```
Router# show interface gigabitethernet4/0
GigabitEthernet4/0 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0087.c08b.4824 (bia
0087.c08b.4824)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  output flow-control is off, input flow-control is on
  0 pause input, 0 pause output
  Full-duplex, 1000Mb/s
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, 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:fifo
  Output queue:0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     398301 packets input, 29528679 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 input packets with dribble condition detected
     790904 packets output, 54653461 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to configure Gigabit Ethernet interface 0/10 as a routed port and to assign it an IP address:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet0/10
Router(config-if)# no switchport
Router(config-if)# ip address 10.1.2.3 255.255.0.0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following is sample output from the **show interfaces** privileged EXEC command for Gigabit Ethernet interface 0/2:

```
Router# show interfaces gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4400 (bia 0002.4b29.4400)
  Internet address is 192.20.135.21/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:08, 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
     89604 packets input, 8480109 bytes, 0 no buffer
     Received 81848 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     60665 packets output, 6029820 bytes, 0 underruns
     0 output errors, 0 collisions, 16 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following is sample output from the **show ip interface** privileged EXEC command for Gigabit Ethernet interface 0/2:

```
Router# show ip interface gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up
  Internet address is 192.20.135.21/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following is sample output from the **show running-config** privileged EXEC command for Gigabit Ethernet interface 0/2:

```
Router# show running-config interface gigabitethernet0/2
Building configuration...

Current configuration : 122 bytes
!
interface GigabitEthernet0/2
 no switchport
 ip address 192.20.135.21 255.255.255.0
 speed 100
 mls qos trust dscp
end
```

Intrachassis Stacking: Example

The following example shows how to stack GE port 2/0 to GE port 3/0 to form an extended VLAN within one chassis:

```
Router# config terminal
Router(config)# interface Gigabit 2/0
Router(config-if)# switchport stacking-link interface Gigabit3/0
```

The following example shows interchassis stacking being verified between GE port 2/0 and GE port 3/0:

```
Router# show interface gigabit 2/0


 GigabitEthernet2/0 is up, line protocol is down
   Internal Stacking Link Active : Gi2/0 is stacked with Gi3/0
   Hardware is Gigabit Ethernet, address is 001b.3f2b.2c24 (bia 001b.3f2b.2c24)
   MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   Full-duplex mode, link type is force-up, media type is unknown 0
   output flow-control is off, input flow-control is off
   Full-duplex, 1000Mb/s
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input 1d22h, output never, output hang never
   Last clearing of "show interface" counters 1d22h
   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
      250707 packets input, 19562597 bytes, 0 no buffer
      Received 7 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 0 multicast, 0 pause input
      0 input packets with dribble condition detected
      7469804 packets output, 582910831 bytes, 0 underruns(0/0/0)
      0 output errors, 0 collisions, 0 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier, 0 pause output
      0 output buffer failures, 0 output buffers swapped out
```

Configuring Switched Port Analyzer (SPAN): Example

The following example shows SPAN session 1 being configured to monitor bidirectional traffic from source interface Fast Ethernet 5/1. Fast Ethernet interface 5/48 is configured as the destination for SPAN session 1 and Fast Ethernet interface 5/2 is removed as a SPAN source for SPAN session 1.

```
Router(config)# monitor session 1 source interface fastethernet 5/1
Router(config)# monitor session 1 destination interface fastethernet 5/48
Router(config)# no monitor session 1 source interface fastethernet 5/2
```

Configuring Layer 3 Interfaces: Example

The following example shows how to configure Gigabit Ethernet interface 0/10 as a routed port and to assign it an IP address:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet0/10
Router(config-if)# no switchport
Router(config-if)# ip address 10.1.2.3 255.255.0.0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following is sample output from the **show interfaces** privileged EXEC command for Gigabit Ethernet interface 0/2:

```
Router# show interfaces gigabitethernet0/2

GigabitEthernet0/2 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4400 (bia 0002.4b29.4400)
  Internet address is 192.20.135.21/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:08, 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
     89604 packets input, 8480109 bytes, 0 no buffer
     Received 81848 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     60665 packets output, 6029820 bytes, 0 underruns
     0 output errors, 0 collisions, 16 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following is sample output from the **show ip interface** privileged EXEC command for Gigabit Ethernet interface 0/2:

```
Router# show ip interface gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up
  Internet address is 192.20.135.21/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following is sample output from the **show running-config** privileged EXEC command for Gigabit Ethernet interface 0/2:

```
Router# show running-config interface gigabitethernet0/2
Building configuration...

Current configuration : 122 bytes
!
interface GigabitEthernet0/2
 no switchport
 ip address 192.20.135.21 255.255.255.0
 speed 100
 mls qos trust dscp
end
```

IGMP Snooping: Example

Default IGMP Snooping Configuration

IGMP snooping is enabled by default on a VLAN or subnet basis. Multicast routing has to be enabled on the router first and then PIM (Multicast routing protocol) has to be enabled on the VLAN interface so that the EtherSwitch network module acknowledges the IGMP join and leave messages that are sent from the hosts connected to the EtherSwitch network module.

```
Router(config)# ip multicast-routing
Router(config-if)# interface VLAN1
Router(config-if)# ip-address 192.168.10.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
```

The following example shows the output from configuring IGMP snooping:

```
Router# show mac-address-table multicast igmp-snooping

Slot # :3
--------------
    MACADDR     VLANID     INTERFACES

0100.5e00.0001    1
0100.5e00.0002    1
0100.5e00.000d    1
0100.5e00.0016    1
0100.5e05.0505    1        Fa3/12
0100.5e06.0606    1        Fa3/13
0100.5e7f.ffff    1        Fa3/13
0100.5e00.0001    2
0100.5e00.0002    2
0100.5e00.000d    2
0100.5e00.0016    2
0100.5e00.0128    2
0100.5e05.0505    2        Fa3/10
0100.5e06.0606    2        Fa3/11
```

The following example shows output from the **show running-config interface** privileged EXEC command for VLAN 1:

```
Router# show running-config interface vlan 1

Building configuration...

Current configuration :82 bytes
!
interface Vlan1
 ip address 192.168.4.90 255.255.255.0
 ip pim sparse-mode
end
```

The following example shows output from the **show running-config interface** privileged EXEC command for VLAN 2:

```
Router# show running-config interface vlan 2

Building configuration...

Current configuration :82 bytes
!
interface Vlan2
 ip address 192.168.5.90 255.255.255.0
 ip pim sparse-mode
end
```

The following example shows output verifying multicasting support:

```
Router# show ip igmp group

IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.255.255.255  Vlan1                    01:06:40  00:02:20  192.168.41.101
224.0.1.40       Vlan2                    01:07:50  00:02:17  192.168.5.90
224.5.5.5        Vlan1                    01:06:37  00:02:25  192.168.41.100
224.5.5.5        Vlan2                    01:07:40  00:02:21  192.168.31.100
224.6.6.6        Vlan1                    01:06:36  00:02:22  192.168.41.101
224.6.6.6        Vlan2                    01:06:39  00:02:20  192.168.31.101
```

The following example shows output from the multicast routing table:

```
Router# show ip mroute

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C -
Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.255), 01:06:43/00:02:17, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:43/00:02:17

(*, 224.0.1.40), 01:12:42/00:00:00, RP 0.0.0.0, flags:DCL
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan2, Forward/Sparse, 01:07:53/00:02:14

(*, 224.5.5.5), 01:07:43/00:02:22, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:40/00:02:22
    Vlan2, Forward/Sparse, 01:07:44/00:02:17

(*, 224.6.6.6), 01:06:43/00:02:18, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:40/00:02:18
    Vlan2, Forward/Sparse, 01:06:43/00:02:16
```

Configuring Fallback Bridging: Examples

This section contains the following examples:

- Creating a Bridge Group: Example, page 213
- Adjusting Spanning Tree Parameters: Example, page 214
- Disabling the Spanning Tree on an Interface: Example, page 214
- Fallback Bridging with DLSW: Example, page 214

Creating a Bridge Group: Example

The following example shows how to create bridge group 10, specify the VLAN-bridge STP to run in the bridge group, and assign an interface to the bridge group. The switch device is prevented from forwarding frames for stations that it has dynamically learned in bridge group 10, and the bridge table aging time is set to 200 seconds. Frames with a MAC address of 0800.cb00.45e9 are forwarded through an interface in bridge group 1.

```
Router(config)# bridge 10 protocol vlan-bridge
Router(config)# interface gigabitethernet0/1
Router(config-if)# no switchport
Router(config-if)# bridge-group 10
Router(config-if)# exit
Router(config)# no bridge 10 acquire
Router(config)# bridge 10 aging-time 200
Router(config)# bridge 1 address 0800.cb00.45e9 forward gigabitethernet0/1
```

Adjusting Spanning Tree Parameters: Example

The following example shows how to set the switch priority to 100 for bridge group 10, how to change the priority of an interface to 20 in bridge group 10, and how to change the path cost on an interface to 20 in bridge group 10. In bridge group 10 the hello interval is changed to 5 seconds, the forward-delay interval is changed to 10 seconds, and the maximum-idle interval to 30 seconds.

```
Router(config)# bridge 10 priority 100
Router(config)# interface gigabitethernet0/1
Router(config-if)# bridge-group 10 priority 20
Router(config-if)# bridge-group 10 path-cost 20
Router(config)# bridge 10 hello-time 5
Router(config)# bridge 10 forward-time 10
Router(config)# bridge 10 max-age 30
```

Disabling the Spanning Tree on an Interface: Example

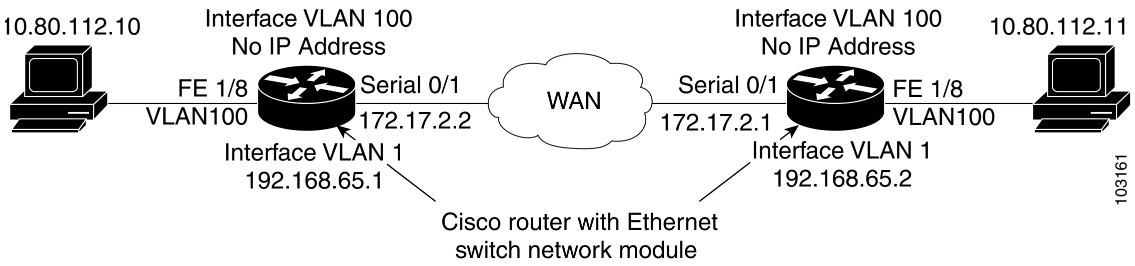
The following example shows how to disable spanning tree on an interface in bridge group 10:

```
Router(config)# interface gigabitethernet0/1
Router(config-if)# bridge group 10 spanning-disabled
```

Fallback Bridging with DLSW: Example

The following example shows how to configure fallback bridging with DLSW on the EtherSwitch network module. Using the network in Figure 24 this example shows how to bridge VLANs over routers. Normally VLANs terminate at a router. Note that both PCs are on the same subnet although they are actually separated by two routers. The fallback bridging creates a virtual bridge between the two PCs.

Figure 24 Fallback Bridging with DLSW Network Example



The following are partial configurations for Router A and Router B:

Router A

```
no spanning-tree vlan 1
no spanning-tree vlan 100
!
bridge irb
!
```

```
dlsw local-peer peer-id 192.168.65.1
dlsw remote-peer 0 tcp 192.168.66.1
dlsw bridge-group 1
!
interface FastEthernet1/8
 switchport access vlan 100
 no ip address
!
interface Vlan1
 ip address 192.168.65.1 255.255.255.0
!
interface Vlan100
 no ip address
 bridge-group 1
 bridge-group 1 spanning-disabled
!
bridge 1 protocol ieee
call rsvp-sync
```

Router B

```
no spanning-tree vlan 1
no spanning-tree vlan 100
!
bridge irb
!
dlsw local-peer peer-id 192.168.66.1
dlsw remote-peer 0 tcp 192.168.65.1
dlsw bridge-group 1
!
interface FastEthernet1/8
 switchport access vlan 100
 no ip address
interface Vlan1
 ip address 192.168.65.2 255.255.255.0
!
interface Vlan100
 no ip address
 bridge-group 1
 bridge-group 1 spanning-disabled
!
bridge 1 protocol ieee
call rsvp-sync
```

Configuring Network Security with ACLs at Layer 2: Examples

Creating Numbered Standard and Extended ACLs: Example

The following example shows how to create a standard ACL to deny access to IP host 171.69.198.102, permit access to any others, and display the results:

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Router(config)# end
Router# show access-lists

Standard IP access list 2
    deny   171.69.198.102
    permit any
```

The following example shows that the switch accepts addresses on network 36.0.0.0 subnets and denies all packets coming from 56.0.0.0 subnets. The ACL is then applied to packets entering Gigabit Ethernet interface 0/1:

```
Router(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Router(config)# access-list 2 deny 56.0.0.0 0.255.255.255
Router(config)# interface gigabitethernet0/1
Router(config-if)# ip access-group 2 in
```

The following example shows how to create and display an extended access list to deny Telnet access from any host in network 171.69.198.0 to any host in network 172.20.52.0 and permit any others (the **eq** keyword after the destination address means to test for the TCP destination port number equaling Telnet):

```
Router(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq 
telnet
Router(config)# access-list 102 permit tcp any any
Router(config)# end
Router# show access-lists

Extended IP access list 102
    deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
    permit tcp any any
```

The following example shows an extended ACL with a network connected to the Internet and any host on the network being able to form TCP Telnet and SMTP connections to any host on the Internet:

```
Router(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Router(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Router(config)# interface gigabitethernet0/1
Router(config-if)# ip access-group 102 in
```

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Because the secure system behind the switch always accepts mail connections on port 25, the incoming services are controlled.

Creating Named Standard and Extended ACLs: Example

The following example shows how you can delete individual ACEs from a named ACL:

```
Router(config)# ip access-list extended border-list
Router(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

The following example shows the marketing_group ACL allowing any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denying any other TCP traffic. It permits any other IP traffic:

```
Router(config)# ip access-list extended marketing_group
Router(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# permit ip any any
```

The ACLs are applied to permit Gigabit Ethernet port 0/1, which is configured as a Layer 2 port, with the marketing_group ACL applied to incoming traffic.

```
Router(config)# interface gigabitethernet0/1
Router(config-if)# ip access-group marketing_group in
```

Including Comments About Entries in ACLs: Example

The following example shows an IP numbered standard ACL using the **access-list** *access-list number* **remark** *remark* global configuration command to include a comment about an access list. In this example, the workstation belonging to Jones is allowed access, and the workstation belonging to Smith is not allowed access:

```
Router(config)# access-list 1 remark Permit only Jones workstation through
Router(config)# access-list 1 permit 171.69.2.88
Router(config)# access-list 1 remark Do not allow Smith workstation through
Router(config)# access-list 1 deny 171.69.3.13
```

The following example shows an entry in a named IP ACL using the **remark** access-list global configuration command to include a comment about an access list. In this example, the Jones subnet is not allowed to use outbound Telnet:

```
Router(config)# ip access-list extended telnetting
Router(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Router(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

In this example of a numbered ACL, the workstation belonging to Jones is allowed access, and the workstation belonging to Smith is not allowed access:

```
Router(config)# access-list 1 remark Permit only Jones workstation through
Router(config)# access-list 1 permit 171.69.2.88
Router(config)# access-list 1 remark Do not allow Smith workstation through
Router(config)# access-list 1 deny 171.69.3.13
```

In this example of a numbered ACL, the Winter and Smith workstations are not allowed to browse the web:

```
Router(config)# access-list 100 remark Do not allow Winter to browse the web
Router(config)# access-list 100 deny host 171.69.3.85 any eq www
Router(config)# access-list 100 remark Do not allow Smith to browse the web
Router(config)# access-list 100 deny host 171.69.3.13 any eq www
```

Applying the ACL to an Interface: Example

The following example shows how to apply access list 2 on Gigabit Ethernet interface 0/3 to filter packets entering the interface:

```
Router(config)# interface gigabitethernet0/3
Router(config-if)# ip access-group 2 in
```

Displaying Standard and Extended ACLs: Example

The following example displays all standard and extended ACLs:

```
Router# show access-lists
```

```
Standard IP access list 1
    permit 172.20.10.10
Standard IP ACL 10
    permit 12.12.12.12
Standard IP access list 12
    deny   1.3.3.2
Standard IP access list 32
    permit 172.20.20.20
Standard IP access list 34
    permit 10.24.35.56
    permit 23.45.56.34
Extended IP access list 120
```

The following example displays only IP standard and extended ACLs:

```
Router# show ip access-lists
Standard IP access list 1
    permit 172.20.10.10
Standard IP access list 10
    permit 12.12.12.12
Standard IP access list 12
    deny   1.3.3.2
Standard IP access list 32
    permit 172.20.20.20
Standard IP access list 34
    permit 10.24.35.56
    permit 23.45.56.34
Extended IP access list 120
```

Displaying Access Groups: Example

You use the **ip access-group** interface configuration command to apply ACLs to a Layer 3 interface. When IP is enabled on an interface, you can use the **show ip interface** *interface-id* privileged EXEC command to view the input and output access lists on the interface, as well as other interface characteristics. If IP is not enabled on the interface, the access lists are not shown.

The following example shows how to view all access groups configured for VLAN 1 and for Gigabit Ethernet interface 0/2:

```
Router# show ip interface vlan 1
GigabitEthernet0/2 is up, line protocol is down
  Internet address is 10.20.30.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is permit Any
  Inbound  access list is 13
.
.
.

Router# show ip interface fastethernet 0/9
FastEthernet0/9 is down, line protocol is down
  Inbound  access list is ip1
```

The only way to ensure that you can view all configured access groups under all circumstances is to use the **show running-config** privileged EXEC command. To display the ACL configuration of a single interface, use the **show running-config interface** *interface-id* command.

The following example shows how to display the ACL configuration of Gigabit Ethernet interface 0/1:

```
Router# show running-config interface gigabitethernet0/1
Building configuration...

Current configuration :112 bytes
!
interface GigabitEthernet0/1
 ip access-group 11 in
 snmp trap link-status
 no cdp enable
end
```

Compiling ACLs: Example

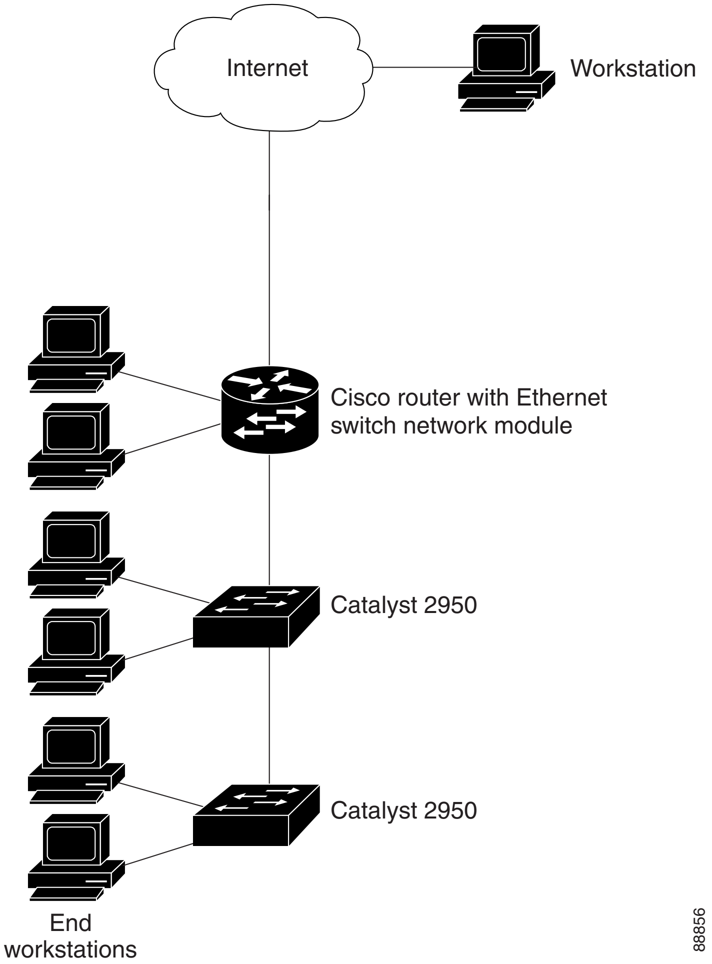
For detailed information about compiling ACLs, refer to the *Security Configuration Guide* and the “IP Services” chapter of the *Cisco IOS IP and IP Routing Configuration Guide.*

Figure 25 shows a small networked office with a stack of Catalyst 2950 switches that are connected to a Cisco router with an EtherSwitch network module installed. A host is connected to the network through the Internet using a WAN link.

Use switch ACLs to do these tasks:

- Create a standard ACL, and filter traffic from a specific Internet host with an address 172.20.128.64.
- Create an extended ACL, and filter traffic to deny HTTP access to all Internet hosts but allow all other types of access.

Figure 25 Using Switch ACLs to Control Traffic



The following example uses a standard ACL to allow access to a specific Internet host with the address 172.20.128.64:

```
Router(config)# access-list 6 permit 172.20.128.64 0.0.0.0
Router(config)# end
Router(config)# interface gigabitethernet0/1
Router(config-if)# ip access-group 6 in
```

The following example uses an extended ACL to deny traffic from port 80 (HTTP). It permits all other types of traffic:

```
Router(config)# access-list 106 deny tcp any any eq 80
Router(config)# access-list 106 permit ip any any
Router(config)# interface gigabitethernet0/2
Router(config-if)# ip access-group 106 in
```

Configuring QoS on the EtherSwitch network module: Examples

- Classifying Traffic by Using ACLs: Example, page 221
- Classifying Traffic by Using Class Maps: Example, page 221

Classifying Traffic by Using ACLs: Example

The following example shows how to allow access for only those hosts on the two specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the ACL statements is rejected.

```
Router(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Router(config)# access-list 1 permit 36.0.0.0 0.0.0.255
```

Classifying Traffic by Using Class Maps: Example

The following example shows how to configure the class map called class1. The class1 has one match criterion, which is an ACL called 103.

```
Router(config)# access-list 103 permit any any tcp eq 80
Router(config)# class-map class1
Router(config-cmap)# match access-group 103
Router(config-cmap)# end
Router#
```

Classifying, Policing, and Marking Traffic by Using Policy Maps: Example

The following example shows how to create a policy map and attach it to an ingress interface. In the configuration, the IP standard ACL permits traffic from network 10.1.0.0. For traffic matching this classification, the DSCP value in the incoming packet is trusted. If the matched traffic exceeds an average traffic rate of 48000 bps and a normal burst size of 8000 bytes, its DSCP is marked down to a value of 10 and transmitted.

```
Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)# class-map ipclass1
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map flow1t
Router(config-pmap)# class ipclass1
Router(config-pmap-c)# police 5000000 8192 exceed-action dscp 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitethernet0/1
Router(config-if)# switchport mode access
Router(config-if)# service-policy input flow1t
```

Configuring the CoS-to-DSCP Map: Example

The following example shows how to modify and display the CoS-to-DSCP map:

```
Router# configure terminal
Router(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
Router(config)# end
Router# show mls qos maps cos-dscp

Cos-dscp map:
        cos:  0  1  2  3  4  5  6  7
     --------------------------------
       dscp:  8  8  8  8 24 32 56 56
```

Configuring the DSCP-to-CoS Map: Example

The following example shows how the DSCP values 26 and 48 are mapped to CoS value 7. For the remaining DSCP values, the DSCP-to-CoS mapping is the default.

```
Router(config)# mls qos map dscp-cos 26 48 to 7
Router(config)# exit

Router# show mls qos maps dscp-cos

Dscp-cos map:
       dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
     -----------------------------------------------
        cos:  0  1  1  2  2  3  7  4  4  5  5  7  7
```

Displaying QoS Information: Example

The following example shows how to display the DSCP-to-CoS maps:

```
Router# show mls qos maps dscp-cos

Dscp-cos map:
       dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
     -----------------------------------------------
        cos:  0  1  1  2  2  3  3  4  4  5  5  6  7
```

Additional References

The following sections provide references related to the EtherSwitch network module.

Related Documents

Related Topic	Document Title
Quick Start Guide for the Cisco 2600 series	*Cisco 2600 Series Modular Routers Quick Start Guide*
Hardware installation for the Cisco 2600 series	*Cisco 2600 Series Hardware Installation Guide*
Quick Start Guide for the Cisco 3600 series	Quick start guides for Cisco 3600 series routers
Hardware installation for the Cisco 3600 series	*Cisco 3600 Series Hardware Installation Guide*
Quick Start Guide for the Cisco 3700 series	Quick start guides for Cisco 3700 series routers
Hardware installation for the Cisco 3700 series	Hardware installation documents for Cisco 3700 series routers
Information about configuring Voice over IP features	*Cisco IOS Voice, Video, and Fax Configuration Guide*
Voice over IP commands	*Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.3 T
Information about Flow Control	*Configuring Gigabit Ethernet Switching*

Standards

Standards	Title
802.1d	*Spanning Tree Protocol*
802.1p	*Supplement to MAC Bridges: Traffic Class Expediting and Dynamic Multicast Filtering*
802.1q	*Virtual LAN (VLAN) Bridges*
802.1x	*Port Based Network Access Control*

MIBs

MIBs	MIBs Link
• IF MIB • CISCO-CDP-MIB • CISCO-CDP-MIB • CISCO-IMAGE-MIB • CISCO-FLASH-MIB • OLD-CISCO-CHASSIS-MIB • CISCO-VTP-MIB • CISCO-HSRP-MIB • OLD-CISCO-TS-MIB • CISCO-ENTITY-ASSET-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-ENTITY-ASSET-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VLAN-IFINDEX-RELATIONSHIP-MIB • RMON1-MIB • PIM-MIB • CISCO-STP-EXTENSIONS-MIB • IPMROUTE-MIB • CISCO-MEMORY-POOL-MIB • CISCO-RTTMON-MIB • CISCO-PROCESS-MIB • CISCO-COPS-CLIENT-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1213	*Management Information Base for Network Management of TCP/IP-Based Internets, MIB-II*
RFC 1253	*OSPF Version 2 Management Information Base*
RFC 1493	*Definitions of Managed Objects for Bridges*
RFC 1643	*Definitions of Managed Objects for the Ethernet-Like Interface Types*
RFC 2037	*Entity MIB using SMIv2*
RFC 2284	*PPP Extensible Authentication Protocol (EAP)*

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.

- **aaa authentication dot1x**
- **class (EtherSwitch)**
- **debug dot1x (EtherSwitch)**
- **debug eswilp**
- **debug ip igmp snooping**
- **debug spanning-tree**
- **dot1x default**
- **dot1x max-req**
- **dot1x multiple-hosts**
- **dot1x port-control**
- **dot1x re-authenticate (EtherSwitch)**
- **dot1x re-authentication**
- **dot1x timeout (EtherSwitch)**
- **ip igmp snooping**
- **ip igmp snooping vlan**
- **ip igmp snooping vlan immediate-leave**
- **ip igmp snooping vlan mrouter**
- **ip igmp snooping vlan static**
- **mls qos cos**
- **mls qos map**
- **mls qos trust**
- **police (EtherSwitch)**
- **show dot1x (EtherSwitch)**
- **show ip igmp snooping**

- **show ip igmp snooping mrouter**
- **show mls masks**
- **show mls qos interface**
- **show mls qos maps**
- **show spanning-tree**
- **show storm-control**
- **spanning-tree backbonefast**
- **storm-control**
- **switchport**

Glossary

802.1d—IEEE standard for MAC bridges.

802.1p—IEEE standard for queuing and multicast support.

802.1q—IEEE standard for VLAN frame tagging.

802.1x—IEEE standard for port-based network access control.

ACE—access control entry. Entry in an access control list.

ACL—access control list. Used for security or as a general means to classify traffic.

AgPort—aggregate port (another name for EtherChannel).

ATM—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3.

authentication server—Entity that validates the credentials of a host trying to obtain access to the network.

authenticator—Entity that enforces authentication rules for hosts connecting to a LAN via one of its ports.

authorization state—The state of a controlled port. It can be authorized (access allowed) or unauthorized (access denied).

AVVID—Architecture for voice, video, and integrated data.

BRI—Basic Rate Interface. ISDN interface comprising two B channels and one D channel for circuit-switched communication of voice, video, and data.

CAC—connection admission control. Set of actions taken by each ATM switch during connection setup to determine whether a connection's requested QoS will violate the QoS guarantees for established connections. CAC is also used when routing a connection request through an ATM network.

candidate—Switch that is not part of a cluster, but is eligible to join a cluster because it meets the qualification criteria of the cluster.

CBWFQ—class-based weighted fair queuing. Extends the standard WFQ functionality to provide support for user-defined traffic classes.

CCN—Cisco Communications Network (Cisco IP phones and IP PBX).

classification—Process of sorting incoming packets by examining fields of interest in the packet header. Fields can be addresses, ports, DSCP value, and so on.

cluster—Group of switches that are managed as a single device. A cluster comprises one commander and multiple members.

cluster commander—Switch that provides the primary management interface to a cluster.

cluster member—Member switch that is managed through the cluster commander.

CoS—class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a session. A CoS definition comprises a virtual route number and a transmission priority field. Also called ToS.

DSCP—differentiated services code point. In QoS, a modification of the type of service byte. Six bits of this byte are being reallocated for use as the DSCP field, where each DSCP specifies a particular per-hop behavior that is applied to a packet.

DSL—digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.

EAP—Extensible Authentication Protocol. A mechanism (originally designed for PPP in RFC 2284) that provides authentication of hosts requesting access to a network.

EAPOL—EAP over LAN.

Frame Relay—The capability to carry normal telephony-style voice over an IP-based network with POTS-like functionality, reliability, and voice quality. VoIP lets a router carry voice traffic (such as telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

FXO—Foreign Exchange Office. An FXO interface connects to the Public Switched Telephone Network (PSTN) central office and is the interface offered on a standard telephone. Cisco's FX interface is an RJ-11 connector that allows an analog connection at the PSTN's central office or to a station interface on a PBX.

FXS—Foreign Exchange Station. An FXS interface connects directly to a standard telephone and supplies ring, voltage, and dial tone. Cisco's FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, keysets, and PBXs.

HSRP—Hot Standby Router Protocol. Provides high network availability and transparent network topology changes. HSRP creates a hot standby router group with a lead router that services all packets sent to the hot standby address. The lead router is monitored by other routers in the group, and if it fails, one of these standby routers inherits the lead position and the hot standby group address.

IGMP—Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

ISL—InterSwitch Link, which is used to carry traffic for multiple VLANs. A method of encapsulating tagged LAN frames and transporting them over a full-duplex, point-to-point Ethernet link. The encapsulated frames can be Token Ring or Fast Ethernet and are carried unchanged from transmitter to receiver.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

policing—Process of ensuring whether a stream of classified incoming packets conforms to a particular traffic profile. An action (drop or remark) is taken based on the rate of arrival of packets.

PRI—primary rate interface. ISDN interface to primary rate access. Primary rate access consists of one 64-kbps D channel and 23 (T1) or 30 (E1) B channels for voice or data. Compare with BRI.

PSTN—public switched telephone network. General term referring to the variety of telephone networks and services in place worldwide. Also called POTS.

PVC—permanent virtual circuit. 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.

PVST—Per-VLAN spanning tree. Support for dot1q trunks to map multiple spanning trees to a single spanning tree.

QoS—quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

RADIUS—Remote Access Dial-In User Service. A service used to authenticate and authorize clients.

RMON—remote monitoring. MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.

RSVP—Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.

SIP—Session Initiation Protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, which was published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.

SNMP—Simple Network Management Protocol. Network 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.

stacking—Connecting two switches so they behave as one entity for management purposes. Regarding an EtherSwitch network module, stacking means connecting two EtherSwitch network modules inside a chassis so that they behave as one switch.

STP—Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, which enables a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange Bridge Protocol Data Unit (BPDU) messages with other bridges to detect loops and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.

supplicant—Entity requesting access to the network via the authenticator.

SVI—Switch Virtual Interface. Represents a VLAN of switch ports as one interface to the routing or bridging function in a system.

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.

VLAN—virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are on separate LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VoIP—Voice over IP. Ability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (such as telephone calls and faxes) over an IP network. In VoIP, the digital signal processor (DSP) segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

VoIPoFR—Voice-over-IP over Frame-Relay.

VPN—virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VQP—VLAN Query Protocol.

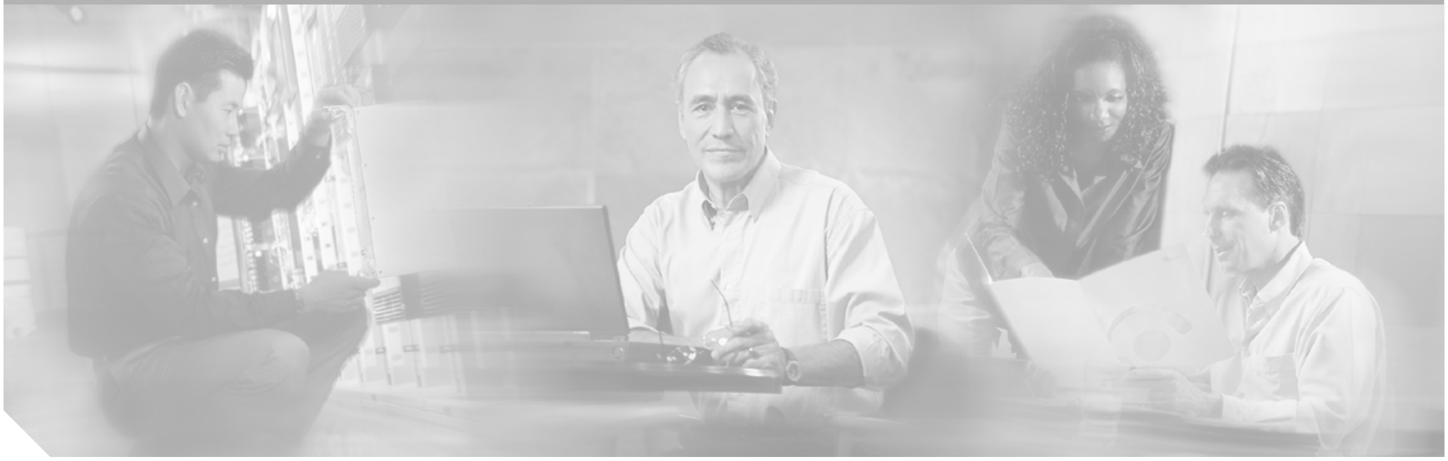
VTP—VLAN Trunking Protocol.

WAN—wide area network. A communications network that covers a wide geographic area such as state or country. A LAN (local-area network) is within a building or complex, and a MAN (metropolitan-area network) generally covers a city or suburb.

WFQ—weighted fair queuing. In QoS, a flow-based queuing algorithm that schedules low-volume traffic first while letting high-volume traffic share the remaining bandwidth. This is handled by assigning a weight to each flow, where lower weights are the first to be serviced.

WRR—Weighted Round-Robin. Type of round-robin scheduling that prevents low-priority queues from being completely neglected during periods of high-priority traffic. The WRR scheduler transmits some packets from each queue in turn. The number of packets it transmits corresponds to the relative importance of the queue.

Note Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.



Part 2: Serial Interfaces

Configuring Serial Interfaces

Use the information in this chapter to configure serial interfaces.

For information on configuring an ATM interface, refer to the "Configuring ATM" chapter in the *Cisco IOS Asynchronous Transfer Mode Configuration Guide*.

For hardware technical descriptions and information about installing interfaces, refer to the hardware installation and configuration publication for your product. For a complete description of serial interface commands used in this chapter, refer to the *Cisco IOS Interface and Hardware Component Command Reference*. To locate documentation of other commands that appear in this chapter, use the master commands list or search online.

To identify the hardware platform or software image information associated with a feature, use Cisco Feature Navigator on Cisco.com to search for information about the feature.

This chapter includes the following sections:

For examples of configuration tasks shown in this chapter, see the "Serial Interface Configuration Examples" section on page 302.

Configuring a High-Speed Serial Interface

The High-Speed Serial Interface (HSSI) Interface Processor (HIP) provides a single HSSI network interface. The network interface resides on a modular interface processor that provides a direct connection between the high-speed CiscoBus and an external network.

The HSSI port adapters (PA-H and PA-2H) are available on:

- Cisco 7200 series routers
- Second-generation Versatile Interface Processors (VIP2s) in Cisco 7500 series routers
- Cisco 7000 series routers with the 7000 series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI)

The PA-H provides one high-speed synchronous serial interface, and the PA-2H provides two high-speed synchronous serial interfaces that support full-duplex and data rates up to 52 Mbps. For more information on the PA-H, refer to the *PA-H HSSI Port Adapter Installation and Configuration* publication. For more information on the PA-2H, refer to the *PA-2H Dual-Port HSSI Port Adapter Installation and Configuration* publication.

The Cisco 3600 series 1-port HSSI network module provides full-duplex connectivity at SONET OC-1/STS-1 (51.840 MHz), T3 (44.736 MHz), and E3 (34.368 MHz) rates in conformance with the EIA/TIA-612 and EIA/TIA-613 specifications. The actual rate of the interface depends on the external data service unit (DSU) and the type of service to which it is connected. This 1-port HSSI network module can reach speeds of up to 52 Mbps in unidirectional traffic with 1548-byte packets and 4250 packets per second. ATM, High-Level Data Link Control (HDLC), PPP, Frame Relay, and Switched Multimegabit Data Service (SMDS) WAN services are all fully supported.

Before you configure the 1-port HSSI network module, complete the following prerequisite tasks:

- Install the HSSI Network Module in a chassis slot. For information on how to install this network module, refer to the "Installing a 1-Port HSSI Network Module in a Chassis Slot" section in the *1-Port HSSI Network Module Configuration Note* publication.
- Complete basic device configuration, including host name, user name, protocol, and security configuration. For more information about basic device configuration, refer to the *Cisco 3620 Installation and Configuration Guide* or the *Cisco 3640 Installation and Configuration Guide*.

HSSI Configuration Task List

To configure a HSSI interface, perform the tasks in the following sections. Each task is identified as either required or optional.

- Specifying a HSSI Interface, page 234 (Required)
- Specifying HSSI Encapsulation, page 235 (Optional)
- Invoking ATM on a HSSI Line, page 235 (Optional)
- Converting HSSI to Clock Master, page 235 (Optional)

Specifying a HSSI Interface

To specify a High-Speed Serial Interface (HSSI) and enter interface configuration mode, use one of the following commands in global configuration mode.

Command	Purpose
`Router(config)# interface hssi number`	Enters interface configuration.
`Router(config)# interface hssi slot/port`	Enters interface configuration for the Cisco 7500 series routers.

Specifying HSSI Encapsulation

The HSSI supports the serial encapsulation methods, except for X.25-based encapsulations. The default method is HDLC. To define the encapsulation method, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# encapsulation {atm-dxi	hdlc	frame-relay	ppp	sdlc-primary	sdlc-secondary	smds}`	Configures HSSI encapsulation.

For information about PPP, refer to the “Configuring Asynchronous SLIP and PPP” and “Configuring Media-Independent PPP and Multilink PPP” chapters in the *Cisco IOS Dial Technologies Configuration Guide*.

Invoking ATM on a HSSI Line

If you have an ATM DSU, you can invoke ATM over a HSSI line. You do so by mapping an ATM virtual path identifier (VPI) and virtual channel identifier (VCI) to a Data Exchange Interface (DXI) frame address. ATM-DXI encapsulation defines a data exchange interface that allows a DTE (such as a router) and a DCE (such as an ATM DSU) to cooperate to provide a User-Network Interface (UNI) for ATM networks.

To invoke ATM over a serial line, use the following commands in interface configuration mode.

	Command	Purpose
Step 1	`Router(config-if)# encapsulation atm-dxi`	Specifies the encapsulation method.
Step 2	`Router(config-if)# dxi map protocol address vpi vci [broadcast]`	Maps a given VPI and VCI to a DXI frame address.

You can also configure the **dxi map** command on a serial interface.

To configure an ATM interface using an ATM Interface Processor (AIP) card, refer to the “Configuring ATM” chapter in the *Cisco IOS Asynchronous Transfer Mode Configuration Guide*.

Converting HSSI to Clock Master

The HSSI network module provides full-duplex connectivity at SONET OC-1/STS-1 (51.840 MHz), T3 (44.736 MHz), and E3 (34.368 MHz) rates in conformance with the EIA/TIA-612 and EIA/TIA-613 specifications. The actual rate of the interface depends on the DSU and the type of service to which it is connected. To convert the HSSI interface into a clock master use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# hssi internal-clock`	Converts the HSSI interface into a 51.84-MHz clock master.

Configuring a Synchronous Serial Interface

Synchronous serial interfaces are supported on various serial network interface cards or systems. These interfaces support full-duplex operation at T1 (1.544 Mbps) and E1 (2.048 Mbps) speeds. Refer to the *Cisco Product Catalog* for specific information regarding platform and hardware compatibility.

Synchronous Serial Configuration Task List

To configure a synchronous serial interface, perform the tasks in the following sections. Each task in the list is identified as either required or optional.

- Specifying a Synchronous Serial Interface, page 236 (Required)
- Specifying Synchronous Serial Encapsulation, page 237 (Optional)
- Configuring PPP, page 238 (Optional)
- Configuring Half-Duplex and Bisync for Synchronous Serial Port Adapters on Cisco 7200 Series Routers, page 238 (Optional)
- Configuring Compression Service Adapters on Cisco 7500 Series Routers, page 239 (Optional)
- Configuring Compression of HDLC Data, page 240 (Optional)
- Configuring Real-Time Transport Protocol Header Compression, page 240 (Optional)
- Configuring the Data Compression AIM, page 240 (Optional)
- Configuring the CRC, page 248 (Optional)
- Using the NRZI Line-Coding Format, page 248 (Optional)
- Enabling the Internal Clock, page 249 (Optional)
- Inverting the Data, page 249 (Optional)
- Inverting the Transmit Clock Signal, page 249 (Optional)
- Setting Transmit Delay, page 250 (Optional)
- Configuring DTR Signal Pulsing, page 250 (Optional)
- Ignoring DCD and Monitoring DSR as Line Up/Down Indicator, page 250 (Optional)
- Specifying the Serial Network Interface Module Timing, page 251 (Optional)
- Specifying G.703 and E1-G.703/G.704 Interface Options, page 251 (Optional)

See the "Serial Interface Configuration Examples" section on page 302 for examples of configuration tasks described in this chapter.

Specifying a Synchronous Serial Interface

To specify a synchronous serial interface and enter interface configuration mode, use one of the following commands in global configuration mode.

Command	Purpose
`Router(config)# interface serial number`	Enters interface configuration mode.
`Router(config)# interface serial slot/port`	Enters interface configuration mode for the Cisco 7200 or Cisco 7500 series routers.

Command	Purpose
`Router(config)# interface serial slot/port-adapter/port`	Enters interface configuration for the Cisco 7500 series routers.

`Router(config)# interface serial slot/port:channel-group`
(Cisco 7000 series)
`Router(config)# interface serial number:channel-group`
(Cisco 4000 series)
	Enters interface configuration for a channelized T1 or E1 interface.

Specifying Synchronous Serial Encapsulation

By default, synchronous serial lines use the High-Level Data Link Control (HDLC) serial encapsulation method, which provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. The synchronous serial interfaces support the following serial encapsulation methods:

- ATM-DXI
- HDLC
- Frame Relay
- PPP
- Synchronous Data Link Control (SDLC)
- SMDS
- Cisco Serial Tunnel (STUN)
- X.25-based encapsulations

To define the encapsulation method, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# encapsulation {atm-dxi | hdlc | frame-relay | ppp | sdlc-primary | sdlc-secondary | smds | stun | x25}`	Configures synchronous serial encapsulation.

Encapsulation methods are set according to the type of protocol or application you configure in the Cisco IOS software.

- ATM-DXI is described in the "Configuring the CRC" section on page 248.
- PPP is described in the "Configuring Media-Independent PPP and Multilink PPP" chapter in the *Cisco IOS Dial Technologies Configuration Guide*.
- ATM, Frame Relay, and X.25 information and configuration steps are described in the *Cisco IOS Asynchronous Transfer Mode Configuration Guide* and the *Cisco IOS Wide-Area Networking Configuration Guide*.
- The remaining encapsulation methods are defined in their respective books and chapters describing the protocols or applications. Serial encapsulation methods are also discussed in the *Cisco IOS Interface and Hardware Component Command Reference*, under the **encapsulation** command.

By default, synchronous interfaces operate in full-duplex mode. To configure an SDLC interface for half-duplex mode, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# half-duplex`	Configures an SDLC interface for half-duplex mode.

Binary synchronous communication (Bisync) is a half-duplex protocol. Each block of transmission is acknowledged explicitly. To avoid the problem associated with simultaneous transmission, there is an implicit role of primary and secondary station. The primary sends the last block again if there is no response from the secondary within the period of block receive timeout.

To configure the serial interface for full-duplex mode, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# full-duplex`	Specifies that the interface can run Bisync using switched RTS signals.

Configuring PPP

To configure PPP, refer to the "Configuring Media-Independent PPP and Multilink PPP" chapter in the *Cisco IOS Dial Technologies Configuration Guide*.

Configuring Half-Duplex and Bisync for Synchronous Serial Port Adapters on Cisco 7200 Series Routers

The synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+) on Cisco 7200 series routers support half-duplex and Bisync. Bisync is a character-oriented data-link layer protocol for half-duplex applications. In half-duplex mode, data is sent one direction at a time. Direction is controlled by handshaking the Request to Send (RST) and Clear to Send (CTS) control lines. These are described in the following sections:

- Configuring Bisync, page 239
- Configuring Half-Duplex Carrier Modes and Timers, page 239

For more information about the PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+ synchronous serial port adapters, refer to the following publications:

- *PA-8T-V35 Synchronous Serial Port Adapter Installation and Configuration*
- *PA-8T-X21 Synchronous Serial Port Adapter Installation and Configuration*
- *PA-8T-232 Synchronous Serial Port Adapter Installation and Configuration*
- *PA-4T+ Synchronous Serial Port Adapter Installation and Configuration*

Configuring Bisync

To configure the Bisync feature on the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+) on Cisco 7200 series routers, refer to the "Block Serial Tunnelling (BSTUN)" section of the "Configuring Serial Tunnel and Block Serial Tunnel" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*. All commands listed in the "Block Serial Tunnelling (BSTUN)" section apply to the synchronous serial port adapters on Cisco 7200 series routers. Any command syntax that specifies an interface *number* supports the Cisco 7200 series *slot/port* syntax.

Configuring Half-Duplex Carrier Modes and Timers

This section describes how to configure the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+) on Cisco 7200 series routers. To configure the half-duplex feature on synchronous serial port adapters, perform the tasks described in the following sections:

- Understanding Half-Duplex DTE and DCE State Machines, page 288
- Changing Between Controlled-Carrier and Constant-Carrier Modes, page 292
- Tuning Half-Duplex Timers, page 293

Configuring Compression Service Adapters on Cisco 7500 Series Routers

The SA-Comp/1 and SA-Comp/4 data compression service adapters (CSAs) are available on:

- Cisco 7200 series routers
- Second-generation Versatile Interface Processors (VIP2s) in Cisco 7500 series routers (CSAs require VIP2 model VIP2-40.)

The SA-Comp/1 supports up to 64 WAN interfaces, and the SA-Comp/4 supports up to 256 WAN interfaces.

On the Cisco 7200 series routers you can optionally specify which CSA the interface uses to perform hardware compression.

You can configure point-to-point compression on serial interfaces that use PPP encapsulation. Compression reduces the size of a PPP frame via lossless data compression. PPP encapsulations support both predictor and Stacker compression algorithms.

Note If the majority of your traffic is already compressed files, do not use compression.

When you configure Stacker compression on Cisco 7200 series routers and on Cisco 7500 series routers, there are three methods of compression: hardware compression, distributed compression, and software compression. Specifying the **compress stac** command with no options causes the router to use the fastest available compression method, as described here:

- If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression).
- If the CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression).
- If the VIP2 is not available, compression is performed in the router's main processor (software compression).

Using hardware compression in the CSA frees the main processor of the router for other tasks. You can also configure the router to use the VIP2 to perform compression by using the **distributed** option on the **compress** command, or to use the main processor of the router by using the **software** option on the **compress** command. If the VIP2 is not available, compression is performed in the main processor of the router.

When compression is performed in software installed in the main processor of the router, it might significantly affect system performance. You should disable compression in the router's main processor if the router CPU load exceeds 40 percent. To display the CPU load, use the **show process cpu** EXEC command.

For instructions on configuring compression over PPP, refer to the "Configuring Media-Independent PPP and Multilink PPP" chapter in the *Cisco IOS Dial Technologies Configuration Guide*.

Configuring Compression of HDLC Data

You can configure point-to-point software compression on serial interfaces that use HDLC encapsulation. Compression reduces the size of a HDLC frame via lossless data compression. The compression algorithm used is a Stacker (LZS) algorithm.

Compression is performed in software and might significantly affect system performance. We recommend that you disable compression if CPU load exceeds 65 percent. To display the CPU load, use the **show process cpu** EXEC command.

If the majority of your traffic is already compressed files, you should not use compression.

To configure compression over HDLC, use the following commands in interface configuration mode.

	Command	Purpose
Step 1	`Router(config-if)#` **`encapsulation hdlc`**	Enables encapsulation of a single protocol on the serial line.
Step 2	`Router(config-if)#` **`compress stac`**	Enables compression.

Configuring Real-Time Transport Protocol Header Compression

Real-time Transport Protocol (RTP) is a protocol used for carrying packetized audio and video traffic over an IP network. RTP is described in RFC 1889, *RTP—A Transport Protocol for Real-Time Applications*. RTP is not intended for data traffic, which uses TCP or UDP (User Datagram Protocol). RTP provides end-to-end network transport functions intended for applications with real-time requirements, such as audio, video, or simulation data over multicast or unicast network services.

For information and instructions for configuring RTP header compression, refer to the "Configuring IP Multicast Routing" part of the *Cisco IOS IP Multicast Configuration Guide*.

Configuring the Data Compression AIM

The data compression Advanced Interface Module (AIM) provides hardware-based compression and decompression of packet data transmitted and received on the serial network interfaces of the Cisco 2600 series router without occupying the Port Module Slot which might otherwise be used for additional customer network ports. Supported are the industry standard Lempel-Ziv Stac (LZS) and Microsoft point-to-point compression (MPPC) compression algorithms over point-to-point protocol (PPP) or Frame Relay. High-level Data Link Control (HDLC) is not supported. The data compression AIM requires Cisco IOS Release 12.0(1)T or later.

The data compression AIM is a daughtercard assembly that attaches directly to the Cisco 2600 motherboard leaving the single network module slot available for other purposes. The data compression AIM supports only serial interfaces using PPP encapsulation with STAC or MPPC compression, or Frame Relay encapsulation with STAC compression. No routing, bridging, or switching performance is impacted by this feature. The data compression AIM module contains a high-performance data compression coprocessor that implements the LZS and MPPC data compression algorithms. The module provides compression support for up to two E1 lines. The module contains a PCI Target/Initiator system bus interface for access into host system memory with minimal Host processor intervention.

To configure the data compression AIM daughtercard assembly, perform the following tasks:

- Configuring PPP Compression, page 241
- Configuring Frame Relay Map Compression, page 242
- Configuring Frame Relay Payload Compression, page 245
- Configuring Diagnostics, page 247

Configuring PPP Compression

Configure your Cisco 2600 access server to use PPP compression. Specify the following information for each serial interface:

- encapsulation type
- compression algorithm
- the CAIM daughtercard to be designated as the source of this algorithm, and the port.

To configure the PPP form of compression, use the following commands, beginning in privileged EXEC mode.

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# interface serial slot/port`	Enters interface configuration mode to configure serial interface 0 on port 0. If you have installed more than one WAN interface card, you have interfaces 0 and 1. Each WAN interface card has a pair of ports, 0 and 1.
Step 3	`Router(config-if)# encapsulation ppp`	Specifies the ppp encapsulation type.[1]
Step 4	`Router(config-if)# compress {mppc stac} caim element-number`	Specifies one of the algorithms (mppc, predictor, or stac) on the CAIM card for port 0.[2]
Step 5	`Router(config-if)# no shutdown`	Restarts the interface.
Step 6	`Router(config-if)# Ctrl-Z`	Returns to EXEC mode.

[1] You also have the option of configuring encapsulation for Frame Relay.

[2] You can also configure compression for another serial port or another CAIM card, depending upon your configuration.

Verifying PPP Compression

To check that the interface is activated, use the **show interfaces serial** *slot/port* command. Notice the highlighted fields in the following example:

```
Router# show interfaces serial 0/0

Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 1.1.1.2/24
  MTU 1500 bytes, BW 2000 Kbit, DLY 20000 usec,
     reliability 255/255, txload 3/255, rxload 50/255
  Encapsulation PPP, loopback not set, keepalive not set
  LCP Open
  Open: IPCP, CCP ==> If two routers have successfully negotiated compression.
  Last input 00:00:04, output 00:00:00, output hang never
  Last clearing of "show interface" counters 1w1d
  Queueing strategy: fifo
  Output queue 0/40, 80 drops; input queue 0/75, 0 drops
  30 second input rate 397000 bits/sec, 40 packets/sec
  30 second output rate 30000 bits/sec, 40 packets/sec
     27859655 packets input, 4176659739 bytes, 0 no buffer
     Received 175145 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     55309592 packets output, 1044865717 bytes, 0 underruns
     0 output errors, 0 collisions, 12 interface resets
     0 output buffer failures, 0 output buffers swapped out
     36 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

To indicate whether compression is active, use the **show compress** command. Notice the highlighted fields in the following example:

```
Router# show compress

 Serial0/0
     Hardware compression enabled
     CSA in slot 0 in use
     Compressed bytes sent:  317862131 bytes   61 Kbits/sec  ratio: 12.870
     Compressed bytes recv:  221975672 bytes   43 Kbits/sec  ratio: 9.194
     restarts: 1
     last clearing of counters: 41252 seconds
```

Tip

- The interface must report being up.
- No errors should be reported.
- Check this interface again after you are sure that traffic is getting to the Cisco 2600 series router and verify that the **Compressed bytes recv** field value changes.

Configuring Frame Relay Map Compression

Configure Frame Relay to map compression on this Data-Link Connection Identifier (DLCI) to use the specified AIM hardware compression on the Cisco 2600 access server. You must specify the following information for each serial interface:

- The protocol, protocol address
- DLCI

- Encapsulation type
- FRF.9 stac compression algorithm

You must also designate the CAIM daughtercard as a source of this algorithm, and the CAIM element number.

To configure the Frame Relay map compression command for operation, use the following commands beginning in privileged EXEC mode.

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# interface serial slot/port`	Enters interface configuration mode to configure the serial interface. If you have installed more than one WAN interface card, you have interfaces 0 and 1. Each WAN interface card has a pair of ports, 0 and 1.
Step 3	`Router(config-if)# encapsulation frame-relay`	Specifies Frame Relay encapsulation.[1]
Step 4	`Router(config-if)# frame-relay map ip ip-address dlci-number broadcast payload-compression frf9 stac caim element-number`	Specifies the stac algorithm on the CAIM card for the port.[2]
Step 5	`Router(config-controller)# no shutdown`	Restarts the interface.
Step 6	`Router(config-if)# Ctrl-Z`	Returns to EXEC mode.

[1] You also have the option of configuring encapsulation for PPP.

[2] You can also configure compression for another serial port or another CAIM card, depending upon your configuration.

Note The **compress ppp** command applied to the PPP compression configuration example above has no equivalent for compression under Frame Relay.

Verifying Frame Relay Map Compression

To check that the interface is activated with proper compression and encapsulation, use the **show interfaces serial** *slot/port* command. Notice the highlighted fields in the following example:

```
Router# show interfaces serial 0/1

Serial0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 1.1.1.2/24
  MTU 1500 bytes, BW 2000 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive not set
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 2743/0, interface broadcasts 2742
  Last input 03:05:57, output 00:00:03, output hang never
  Last clearing of "show interface" counters 1w1d
  Queueing strategy: fifo
  Output queue 0/40, 80 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     30800054 packets input, 3488155802 bytes, 0 no buffer
     Received 199567 broadcasts, 0 runts, 0 giants, 0 throttles
     2 input errors, 0 CRC, 2 frame, 0 overrun, 0 ignored, 0 abort
     58246738 packets output, 1325052697 bytes, 0 underruns
     0 output errors, 0 collisions, 15 interface resets
     0 output buffer failures, 0 output buffers swapped out
     36 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

To indicate whether compression is active, use the **show controllers serial 1/0** command. Notice the highlighted fields in the following example:

```
Router# show controllers serial 1/0

CD2430 Slot 1, Port 0, Controller 0, Channel 0, Revision 14
Channel mode is synchronous serial
idb 0x811082E8, buffer size 1524, X.21 DTE cable

Global registers
  rpilr 0x2, rir 0x0, risr 0x0, rfoc 0x0, rdr 0x30
  tpilr 0x1, tir 0x0, tisr 0x60, tftc 0x0, tdr 0x41
  mpilr 0x3, mir 0x2, misr 0x60
  bercnt 0xFF, stk 0x0

Per-channel registers for channel 0
  Option registers
  0x02 0x00 0x42 0xE7 0xE0 0x00 0x00
  Command and status registers
  cmr 0xC0, ccr 0x00, csr 0xAC, msvr-rts 0xF1, msvr-dtr 0xF1
  Clock option registers
  rcor 0x06, rbpr 0x01, tcor 0xC8, tbpr 0x01
  Interrupt registers
  ier 0x89, livr 0x00, licr 0x00
  DMA buffer status 0x27
  DMA receive registers
  arbaddr 0x2549D44, arbcnt 1548, arbsts 0x1
  brbaddr 0x2548344, brbcnt 1548, brbsts 0x1
  rcbaddr 0x2549D94
  DMA transmit registers
  atbaddr 0x257F93E, atbcnt 104, atbsts 0x43
  btbaddr 0x25B25C2, btbcnt 1490, btbsts 0x43
  tcbaddr 0x25B25D2
  Special character registers
  schr1 0x00, schr2 0x00, schr3 0x00, schr4 0x00
  scrl 0x0, scrh 0x0, lnxt 0xF1

Driver context information
  Context structure 0x8110D830, Register table 0x40800400
  Serial Interface Control 5:1 Register (0x40800802) is 0x0
  Adaptor Flags 0x0
  Serial Modem Control Register (0x40800804) is 0x18
  Receive static buffer 0x810E1274
  Receive particle buffers 0x8110DE00, 0x8110DDC0
  Transmit DMA buffers 0x8113E240, 0x810F2808, 0x810D4C00, 0x810EA0DC
  Transmit packet with particles 0x0, first word is 0x0
  Interrupt rates (per second) transmit 25, receive 139, modem 0
  True fast-switched packets    41
  Semi fast-switched packets    13449573
  Transmitter hang count        0
  Residual indication count     0
  Bus error count       0
  Aborted short frames count    0
  CRC short frames count        0
Error counters
  CTS deassertion failures      0
  Nested interrupt errors transmit 0, receive 0, modem 0
```

```
Using Compression AIM 0
CompressionAim0
    ds:0x8113FC04 idb:0x8113A6CC
       5005867 uncomp paks in -->      5005867 comp paks out
      38397501 comp paks in   -->     38397502 uncomp paks out
    2882277146 uncomp bytes in-->    497476655 comp bytes out
    3500965085 comp bytes in  -->   1211331227 uncomp bytes out
            72 uncomp paks/sec in-->        72 comp paks/sec out
           557 comp paks/sec in  -->       557 uncomp paks/sec out
        334959 uncomp bits/sec in-->     57812 comp bits/sec out
        406855 comp bits/sec in  -->    140827 uncomp bits/sec out
    68841 seconds since last clear
    holdq:0  hw_enable:1  src_limited:0  num cnxts:8
    no data:0  drops:0  nobuffers:0  enc adj errs:0  fallbacks:
5322165
    no Replace:0  num seq errs:0  num desc errs:0  cmds complete:
43403738
    Bad reqs:0  Dead cnxts:0  No Paks:0  enq errs:0
    rx pkt drops:0  tx pkt drops:0  dequeues:0  requeues:0
    drops disabled:0  clears:0  ints:41973007  purges:203200
    no cnxts:0  bad algos:0  no crams:0  bad paks:0
    # opens:0  # closes:4  # hangs:0
    # 9711 fatal:0  # poison pkts:0  cmd/res ovruns:0
    # dma fatal:0
    Jupiter DMA Controller Registers:(0x40200000
        Cmd Ring:0x025BAE60  Src Ring:0x025BBB60
        Res Ring:0x025BB4E8  Dst Ring:0x025BBDA8
        Status/Cntl:present:0x8080989C  last int:0x9898989C
        Inten:0x30302021  config:0x00080003
        Num DMA ints:41973355
    Hifn9711 Data Compression Coprocessor Registers (0x40201000):
        Config:0x000051D4  Inten:0x00000E00
        Status:0x00004000  FIFO status:0x00004000
        FIFO config:0x00000101
```

Tip

- The interface must report being up.
- No errors should be reported.
- Check this interface again after you are sure that traffic is getting to the Cisco 2600 series router and verify that the **Compressed bytes recv** field value changes.

Configuring Frame Relay Payload Compression

To configure Frame Relay payload compression, use the following commands beginning in privileged EXEC mode.

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`interface serial`** *`slot`***`/`***`port`*	Enters interface configuration mode to configure the specified serial interface and port.

	Command	Purpose
Step 3	`Router(config-if)#` **`encapsulation ppp`**	Specifies PPP encapsulation.[1]
Step 4	`Router(config-if)#` **`frame-relay payload-compression frf9 stac caim`** *`element-number`*	Specifies the stac algorithm on the CAIM card for the specified port.[2]
Step 5	`Router(config-if)#` **`no shutdown`**	Restarts the interface.
Step 6	`Router(config-if)#` **`Ctrl-Z`**	Returns to EXEC mode.

[1] You also have the option of configuring encapsulation for Frame Relay.

[2] You can configure compression for any serial port or another CAIM card, depending upon your configuration.

Verifying Frame Relay Payload Compression

To check that the interface is activated with proper compression and encapsulation, use the **show interfaces serial** *slot/port* command. Notice the highlighted fields in the following example:

```
Router# show interfaces serial 0/0

Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 1.1.1.2/24
  MTU 1500 bytes, BW 2000 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive not set
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 2743/0, interface broadcasts 2742
  Last input 03:05:57, output 00:00:03, output hang never
  Last clearing of "show interface" counters 1w1d
  Queueing strategy: fifo
  Output queue 0/40, 80 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     30800054 packets input, 3488155802 bytes, 0 no buffer
     Received 199567 broadcasts, 0 runts, 0 giants, 0 throttles
     2 input errors, 0 CRC, 2 frame, 0 overrun, 0 ignored, 0 abort
     58246738 packets output, 1325052697 bytes, 0 underruns
     0 output errors, 0 collisions, 15 interface resets
     0 output buffer failures, 0 output buffers swapped out
     36 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Note FRAME-RELAY is not displayed using the **show compress** command. Use the **debug compress** command to see this information.

Tip

- The interface must report being up.
- No errors should be reported.

Configuring Diagnostics

Configure the AIM daughtercard to provide compression for the Cisco 2600 series router. You must specify the following information for each daughtercard installed.

To configure the PPP for compression, use the following commands beginning in user EXEC mode.

	Command	Purpose
Step 1	`Router>` **`enable`**	Enables higher privilege levels, such as privileged EXEC mode.
Step 2	`Router#` **`show pas caim stats`** *`element-number`*	Displays compression statistics for your CAIM.
Step 3	`Router#` **`show compress`**	Displays the current configuration for compression on your Cisco 2600.
Step 4	`Router#` **`clear compress`**	Clears all the counters and resets the CAIM hardware.
Step 5	`Router#` **`show pas caim stats`** *`element-number`*	Displays compression statistics for your CAIM.
Step 6	`Router#` **`Ctrl-Z`**	Returns to EXEC mode.

Verifying Diagnostics

To check that the data compression AIM is collecting statistics that represent proper compression, use the **show pas caim stats** *element-number* command:

```
Router# show pas caim stats 0

CompressionAim0
      ds:0x80F56A44 idb:0x80F50DB8
          422074 uncomp paks in -->       422076 comp paks out
          422071 comp paks in   -->       422075 uncomp paks out
       633912308 uncomp bytes in-->     22791798 comp bytes out
        27433911 comp bytes in  -->    633911762 uncomp bytes out
             974 uncomp paks/sec in-->       974 comp paks/sec out
             974 comp paks/sec in  -->       974 uncomp paks/sec out
        11739116 uncomp bits/sec in-->    422070 comp bits/sec out
          508035 comp bits/sec in  -->  11739106 uncomp bits/sec out
      433 seconds since last clear
      holdq: 0  hw_enable: 1  src_limited: 0  num cnxts: 4
      no data: 0  drops: 0  nobuffers: 0  enc adj errs: 0  fallbacks: 0
      no Replace: 0  num seq errs: 0  num desc errs: 0  cmds complete: 844151
      Bad reqs: 0  Dead cnxts: 0  No Paks: 0  enq errs: 0
      rx pkt drops: 0  tx pkt drops: 0  dequeues: 0  requeues: 0
      drops disabled: 0  clears: 0  ints: 844314  purges: 0
      no cnxts: 0  bad algos: 0  no crams: 0  bad paks: 0
      # opens: 0  # closes: 0 # hangs: 0
```

To identify compression characteristics for each port, use the **show compress** command:

```
Router# show compress

 Serial0/0
     Hardware compression enabled
     CSA in slot 0 in use
     Compressed bytes sent:  317862131 bytes   61 Kbits/sec  ratio: 12.870
     Compressed bytes recv:  221975672 bytes   43 Kbits/sec  ratio: 9.194
     restarts: 1
     last clearing of counters: 41252 seconds
 Serial0/1
     Hardware compression enabled
     CSA in slot 0 in use
     Compressed bytes sent:     249720 bytes    0 Kbits/sec  ratio: 5.923
     Compressed bytes recv:  465843659 bytes   43 Kbits/sec  ratio: 9.128
     restarts: 1
     last clearing of counters: 85525 seconds
```

To reset the CAIM hardware to 0, use the **clear compress** command. There is no output for this command; instead, check the output from the **show compress** command to verify the result:

```
Router# clear compress
Router# show compress

 Serial0/0
     Hardware compression enabled
     CSA in slot 0 in use
     Compressed bytes sent:  0 bytes   61 Kbits/sec  ratio: 0
     Compressed bytes recv:  0 bytes   43 Kbits/sec  ratio: 0
     restarts: 0
     last clearing of counters: 0 seconds
```

Tip

- The interface must report being up.
- No errors should be reported.

Configuring the CRC

The cyclic redundancy check (CRC) on a serial interface defaults to a length of 16 bits. To change the length of the CRC to 32 bits on an Fast Serial Interface Processor (FSIP) or HSSI Interface Processor (HIP) of the Cisco 7500 series only, use the following command in interface configuration mode.

Command	Purpose
`Router (config-if)# crc size`	Sets the length of the CRC.

Using the NRZI Line-Coding Format

The nonreturn-to-zero (NRZ) and nonreturn-to-zero inverted (NRZI) formats are supported on:

- All FSIP interface types on Cisco 7500 series routers
- PA-8T and PA-4T+ synchronous serial port adapters on:
  - Cisco 7000 series routers with RSP7000
  - Cisco 7200 series routers
  - Cisco 7500 series routers

NRZ and NRZI are line-coding formats that are required for serial connections in some environments. NRZ encoding is most common. NRZI encoding is used primarily with EIA/TIA-232 connections in IBM environments.

The default configuration for all serial interfaces is NRZ format. The default is **no nrzi-encoding**.

To enable NRZI format, use one of the following commands in interface configuration mode.

Command	Purpose
`Router(config-if)# nrzi-encoding` or	Enables NRZI encoding format.
`Router(config-if)# nrzi-encoding [mark]`	Enables NRZI encoding format for Cisco 7200 series routers and Cisco 7500 series routers.

Enabling the Internal Clock

When a DTE does not return a transmit clock, use the following interface configuration command on the Cisco 7000 series to enable the internally generated clock on a serial interface:

Command	Purpose
`Router(config-if)# transmit-clock-internal`	Enables the internally generated clock on a serial interface.

Inverting the Data

If the interface on the PA-8T and PA-4T+ synchronous serial port adapters is used to drive a dedicated T1 line that does not have B8ZS encoding, you must invert the data stream on the connecting CSU/DSU or on the interface. Be careful not to invert data on both the CSU/DSU and the interface because two data inversions will cancel each other out.

If the T1 channel on the CT3IP is using alternate mark inversion (AMI) line coding, you must invert the data. For more information, refer to the **t1 linecode** controller configuration command. For more information on the CT3IP, see the "Configuring a Channelized T3 Interface Processor" section on page 253.

To invert the data stream, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# invert data`	Inverts the data on an interface.

Inverting the Transmit Clock Signal

Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE clock) can experience high error rates when operating at the higher transmission speeds. For example, if the interface on the PA-8T and PA-4T+ synchronous serial port adapters is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock signal can correct this shift. To invert the clock signal, use the following commands in interface configuration mode.

Command	Purpose
`Router(config-if)# invert txclock`	Inverts the clock signal on an interface.
`Router(config-if)# invert rxclock`	Inverts the phase of the RX clock on the UIO serial interface, which does not use the T1/E1 interface.

Setting Transmit Delay

It is possible to send back-to-back data packets over serial interfaces faster than some hosts can receive them. You can specify a minimum dead time after transmitting a packet to remove this condition. This setting is available for serial interfaces on the MCI and SCI interface cards and for the HSSI or MIP. Use one of the following commands, as appropriate for your system, in interface configuration mode.

Command	Purpose
`Router(config-if)# transmitter-delay microseconds`	Sets the transmit delay on the MCI and SCI synchronous serial interfaces.
`Router(config-if)# transmitter-delay hdlc-flags`	Sets the transmit delay on the HSSI or MIP.

Configuring DTR Signal Pulsing

You can configure pulsing dedicated Token Ring (DTR) signals on all serial interfaces. When the serial line protocol goes down (for example, because of loss of synchronization), the interface hardware is reset and the DTR signal is held inactive for at least the specified interval. This function is useful for handling encrypting or other similar devices that use the toggling of the DTR signal to reset synchronization. To configure DTR signal pulsing, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# pulse-time seconds`	Configures DTR signal pulsing.

Ignoring DCD and Monitoring DSR as Line Up/Down Indicator

This task applies to:

- Quad Serial NIM (network interface module) interfaces on the Cisco 4000 series
- Hitachi-based serial interfaces on the Cisco 2500 series and Cisco 3000 series

By default, when the serial interface is operating in DTE mode, it monitors the Data Carrier Detect (DCD) signal as the line up/down indicator. By default, the attached DCE device sends the DCD signal. When the DTE interface detects the DCD signal, it changes the state of the interface to up.

In some configurations, such as an SDLC multidrop environment, the DCE device sends the Data Set Ready (DSR) signal instead of the DCD signal, which prevents the interface from coming up. To tell the interface to monitor the DSR signal instead of the DCD signal as the line up/down indicator, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# ignore-dcd`	Configures the serial interface to monitor the DSR signal as the line up/down indicator.

Caution Unless you know for certain that you really need this feature, be very careful using this command. It will hide the real status of the interface. The interface could actually be down and you will not know by looking at show displays.

Specifying the Serial Network Interface Module Timing

On Cisco 4000 series routers, you can specify the serial Network Interface Module timing signal configuration. When the board is operating as a DCE and the DTE provides terminal timing (SCTE or TT), you can configure the DCE to use SCTE from the DTE. When running the line at high speeds and long distances, this strategy prevents phase shifting of the data with respect to the clock.

To configure the DCE to use SCTE from the DTE, use the following command in interface configuration mode.

Command	Purpose

`Router(config-if)#`
`dce-terminal-timing enable`
	Configures the DCE to use SCTE from the DTE.

When the board is operating as a DTE, you can invert the TXC clock signal it gets from the DCE that the DTE uses to transmit data. Invert the clock signal if the DCE cannot receive SCTE from the DTE, the data is running at high speeds, and the transmission line is long. Again, this prevents phase shifting of the data with respect to the clock.

To configure the interface so that the router inverts the TXC clock signal, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# dte-invert-txc`	Specifies timing configuration to invert TXC clock signal.

Specifying G.703 and E1-G.703/G.704 Interface Options

This section describes the optional tasks for configuring a G.703 serial interface (a serial interface that meets the G.703 electrical and mechanical specifications and operates at E1 data rates). G.703 interfaces are available on port adapters for the Fast Serial Interface Processor (FSIP) on a Cisco 4000 series or Cisco 7500 series router.

The E1-G.703/G.704 serial port adapters (PA-4E1G-120 and PA-4E1G-75) are available on:

- Cisco 7500 series routers
- Cisco 7200 series routers
- Cisco 7000 series routers with the 7000 series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI)

These port adapters provide up to four E1 synchronous serial interfaces, which are compatible with and specified by G.703/G.704. The PA-4E1G-120 supports balanced operation, and the PA-4E1G-75 supports unbalanced operation with 15-pin, D-shell (DB-15) receptacles on the port adapters. Both port adapters operate in full-duplex mode at the E1 speed of 2.048 Mbps.

Configuration tasks are described in the following sections:

- Enabling Framed Mode, page 252
- Enabling CRC4 Generation, page 252
- Using Time Slot 16 for Data, page 252
- Specifying a Clock Source, page 252

Enabling Framed Mode

G.703 interfaces have two modes of operation: framed and unframed. By default, G.703 serial interfaces are configured for unframed mode. To enable framed mode, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`timeslot`** *`start-slot`* **–** *`stop-slot`*	Enables framed mode.

To restore the default, use the **no** form of this command or set the starting time slot to 0.

Enabling CRC4 Generation

By default, the G.703 CRC4, which is useful for checking data integrity while operating in framed mode, is not generated. To enable generation of the G.703 CRC4, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`crc4`**	Enables CRC4 generation.

Using Time Slot 16 for Data

By default, time slot 16 is used for signaling. It can also be used for data (in order to get all possible subframes or time slots when in framed mode). To specify the use of time slot 16 for data, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`ts16`**	Specifies that time slot 16 is used for data.

Specifying a Clock Source

A G.703 interface can clock its transmitted data either from its internal clock or from a clock recovered from the receive data stream of the line. By default, the interface uses the receive data stream of the line. To control which clock is used, use the following command in interface configuration mode.

Command	Purpose
Router(config-if)# **clock source** {**line** | **internal** | **loop-timed**}	Specifies the clock used for transmitted data.

Configuring a Channelized T3 Interface Processor

The Channelized T3 Interface Processor (CT3IP) is available on:

- Cisco 7500 series routers
- Cisco 7000 series routers with the 7000 series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI)

The Channelized T3 (CT3) feature board is available on Cisco AS5800 access servers.

These cards provide for the aggregation of channelized interfaces into a single T3 facility. T3 support on the Cisco AS5800 allows support for 28 T1s (672 channels) per chassis. The Channelized T3 dual-wide port adapter (PA-CT3/4T1) can be used in Cisco 7200 series routers.

Note Throughout this document are references to the CT3IP. However, the term CT3IP also applies to the PA-CT3/4T1 and to the CT3 feature board. Wherever you see a description of a feature of the CT3IP, the feature is also available in the PA-CT3/4T1 and the CT3 feature board, unless otherwise indicated.

The CT3IP is a fixed-configuration interface processor based on the second-generation Versatile Interface Processor (VIP2). The CT3 channelized port adapter (PA-CT3/4T1) is a dual-wide port adapter. The CT3IP or PA-CT3/4T1 has four T1 connections via DB-15 connectors and one DS3 connection via BNC connectors. Each DS3 interface can provide up to 28 T1 channels (a single T3 group). Each channel is presented to the system as a serial interface that can be configured individually. The CT3IP or PA-CT3/4T1 can transmit and receive data bidirectionally at the T1 rate of 1.536 Mbps. The four T1 connections use 100-ohm twisted-pair serial cables to external channel service units (CSUs) or to a MultiChannel Interface Processor (MIP) on the same router or on another router. For wide-area networking, the CT3IP or PA-CT3/4T1 can function as a concentrator for a remote site.

Note The VIP2-50 is the newest and fastest second-generation Versatile Interface Processor (VIP2) available on Cisco 7500 series routers that use the Route Switch Processor (RSP), and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). The VIP2-50 provides significantly greater packet and program memory space and increased distributed switching performance.

For more information on the VIP2-50, refer to the *Second-Generation Versatile Interface Processor (VIP2) Installation, Configuration, and Maintenance* publication.

As mentioned above, the CT3IP or PA-CT3/4T1 provides 28 T1 channels for serial transmission of data. Each T1 channel can be configured to use a portion of the T1 bandwidth or the entire T1 bandwidth for data transmission. Bandwidth for each T1 channel can be configured for *n* x 56 kbps or *n* x 64 kbps (where *n* is 1 to 24). The unused portion of the T1 bandwidth, when not running at full T1 speeds, is filled with idle channel data. The CT3IP or PA-CT3/4T1 does not support the aggregation of multiple T1 channels (called *inverse muxing* or *bonding*) for higher bandwidth data rates.

The first three T1 channels of the CT3IP or PA-CT3/4T1 can be broken out to the three DSUP-15 connectors on the CPT3IP or PA-CT3/4T1 so that the T1 can be further demultiplexed by the MIP on the same router or on another router or by other multiplexing equipment. When connecting to the MIP, you configure a channelized T1 as described in the "Configuring External T1 Channels" section on page 258. This is referred to as an external T1 channel.

The CT3IP supports RFC 1406, *Definitions of Managed Objects for DS1 and E1 Interface Types*, and RFC 1407, *DS3 MIB Variables* (CISCO-RFC-1407-CAPABILITY.my). For information about Cisco MIBs, refer to the current Cisco IOS release note for the location of the MIB online reference.

For RFC 1406, Cisco supports all tables except the "Frac" table. For RFC 1407, Cisco supports all tables except the "FarEnd" tables.

The CT3IP supports the following WAN protocols:

- Frame Relay
- HDLC
- PPP
- SMDS Data Exchange Interface (DXI)

The CT3IP meets ANSI T1.102-1987 and BELCORE TR-TSY-000499 specifications for T3 and meets ANSI 62411 and BELCORE TR499 specifications for T1. The CT3IP provides internal CSU functionality and includes reporting performance data statistics, transmit and receive statistics, and error statistics. The CT3IP supports RFC 1406 (T1 MIB) and RFC 1407 (T3 MIB).

External T1 channels do not provide CSU functionality and must connect to an external CSU.

Channelized T3 Configuration Task List

To configure the CT3IP, perform the tasks in the following sections. Each task is identified as either required or optional.

- Configuring T3 Controller Support for the Cisco AS5800, page 255 (Optional)
- Configuring the T3 Controller, page 255 (Optional)
- Configuring Each T1 Channel, page 256 (Required)
- Configuring External T1 Channels, page 258 (Optional)
- Monitoring and Maintaining the CT3IP, page 260 (Optional)
- Verifying T3 Configuration, page 260 (Optional)
- Configuring Maintenance Data Link Messages, page 261 (Optional)
- Enabling Performance Report Monitoring, page 261 (Optional)
- Configuring for BERT on the Cisco AS5300, page 261 (Optional)
- Verifying BERT on the Cisco AS5300, page 262 (Optional)
- Enabling a BERT Test Pattern, page 262 (Optional)
- Enabling Remote FDL Loopbacks, page 263 (Optional)
- Configuring T1 Cable Length and T1/E1 Line Termination, page 263 (Optional)

After you configure the T1 channels on the CT3IP, you can continue configuring it as you would a normal serial interface.

For CT3IP configuration examples, see the "Channelized T3 Interface Processor Configuration Examples" section on page 303.

Configuring T3 Controller Support for the Cisco AS5800

To configure T3 controller support specifically for the CT3 feature board in a Cisco AS5800 access server, use the following commands beginning in user EXEC mode.

	Command	Purpose
Step 1	Router> **enable** Password: *password* Router#	Enters privileged EXEC mode.
Step 2	Router# **configure terminal** Enter configuration commands, one per line. End with **Ctrl-Z**. Router(config)#	Enters global configuration mode.
Step 3	Router(config)# **controller t3** *shelf***/***slot*/**0**	Enters controller configuration mode and specifies a shelf, slot, and port for the T3 controller. 0 is the only valid port value.
Step 4	Router(config-controller)# **description** *ascii-string*	Allows the user to enter a description of the T3 controller.
Step 5	Router(config-controller)# **cablelength** *number*	Specifies a controller **cablelength** value from 0 to 450 (feet).
Step 6	Router(config-controller)# **framing** {**c-bit** | **m23**}	Specifies the type of T3 framing used: **C-bit** specifies c-bit parity framing; **m23** (the default) specifies M23 multiplexer framing.
Step 7	Router(config-controller)# **t1** *ds1* **controller**	Creates a logical T1 controller from each of the specified T3 line time slots. *ds1* is a T1 time slot within the T3 line with a value from 1 to 28. (The T1 controller is in *shelf***/***slot***/**0**:**ds1.)
Step 8	Router(config-controller)# **exit**	Exits controller configuration mode and returns to global configuration mode.
Step 9	Router(config)# **controller t1** *shelf***/***slot***/***port***:***t1-num*	Enters controller configuration mode and specifies a port for the T1 controller. *t1-num* is a T1 time slot within the T3 line with a value from 1 to 28.
Step 10	Router(config-controller)# **exit**	Exits controller configuration mode and returns to global configuration mode.
Step 11	Router(config)# **dial-tdm-clock priority** *number* {**external** | **trunk-slot** *number*} **ds3-port 0 port** *number*	Configures clock priority, which is a value from 1 to 50. Specifies a clocking source: either the **external** reference clock or any port of a **trunk** card. If you are using the external reference clock, no other CLI is needed. If you are using a trunk card, select a dial shelf slot from 0 to 5. Specifies a T3 port number, which has a value of 0. Possible T1 port values are from 1 to 28.
Step 12	Router(config)# **Ctrl-Z**	Returns to EXEC mode.
Step 13	Router# **copy running-config startup-config**	Saves your changes.

Configuring the T3 Controller

If you do not modify the configuration of the CT3IP, the configuration defaults shown in Table 19 are used.

Table 19 CT3IP Controller Defaults

Attribute	Default Value
Framing	auto-detect
Cable length	224 feet
Clock source	internal

If you must change any of the default configuration attributes, use the following commands beginning in global configuration mode.

Command	Purpose
`Router(config)# controller t3 slot/port-adapter/port`	Selects the CT3IP and enters controller configuration mode. The port adapter and port numbers for the CT3IP are 0.
`Router(config-controller)# framing {c-bit | m23 | auto-detect}`	(Optional) Changes the framing format.
`Router(config-controller)# cablelength feet`	(Optional) Changes the cable length (values are 0 to 450 feet). Although you can specify a cable length from 0 to 450 feet, the hardware only recognizes two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.
`Router(config-controller)# clock source {internal | line}`	(Optional) Changes the clock source used by the T3 controller.

Configuring Each T1 Channel

You must configure the time slots used by each T1 channel on the CT3IP. Optionally, you can specify the speed, framing format, and clock source used by each T1 channel. If you do not specify the speed, framing format, and clock source used by each T1 channel, the configuration defaults shown in Table 20 are used.

Table 20 CT3IP T1 Channel Defaults

Attribute	Default Value
Speed	64 kbps
Framing	esf
Clock source	internal
Linecode	b8zs
T1 yellow alarm	detection and generation

To specify the time slots used by each T1 channel, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)# controller t3 slot/port-adapter/port`	Selects the CT3IP and enters controller configuration mode.
Step 2	`Router(config-controller)# t1 channel timeslot range [speed {56 | 64}]`	Configures the time slots (values are 1 to 24) for the T1 channel (values are 1 to 28) and optionally specifies the speed for each T1 channel.

Note The 56-kbps speed is valid only for T1 channels 21 through 28.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

If you need to change any of the default configuration attributes, use the following commands, beginning in global configuration mode.

Command	Purpose
`Router(config)# controller t3 slot/port-adapter/port`	Selects the CT3IP and enters controller configuration mode.
`Router(config-controller)# t1 channel framing {esf | sf}`	(Optional) Changes the framing format used by the T1 channel (values are 1 to 28). If you select **sf** framing, disable yellow alarm detection because the yellow alarm can be incorrectly detected with **sf** framing.
`Router(config-controller)# no t1 channel yellow {detection | generation}`	(Optional) Disables detection or generation of a yellow alarm on the T1 channel (values are 1 to 28).
`Router(config-controller)# t1 channel clock source {internal | line}`	(Optional) Changes the clock source used by the T1 channel (values are 1 to 28).
`Router(config-controller)# t1 channel linecode {ami | b8zs}`	(Optional) Changes the line coding used by the T1 channel (values are 1 to 28). If you select **ami** line coding, you must also invert the data on the T1 channel by using the **invert data** interface command. To do so, first use the **interface serial** *slot***/***port-adapter***/***port***:***t1-channel* global configuration command to select the T1 channel and enter interface configuration mode.

After you configure the T1 channels on the CT3IP, you can continue configuring it as you would a normal serial interface. All serial interface commands might not be applicable to the T1 channel. For more information, see the "Configuring a Synchronous Serial Interface" section on page 236.

To enter interface configuration mode and configure the serial interface that corresponds to a T1 channel, use the following command in global configuration mode.

Command	Purpose
`Router(config)# interface serial slot/port-adapter/port:t1-channel`	Defines the serial interface for a T1 channel (values are 1 to 28) and enters interface configuration mode. The port adapter and port numbers for the CT3IP are 0.

In addition to the commands in the "Configuring a Synchronous Serial Interface" section on page 236, the **invert data** interface command can be used to configure the T1 channels on the CT3IP. If the T1 channel on the CT3IP is using AMI line coding, you must invert the data. For information on the **invert data** interface command, see the "Inverting the Data" section on page 249. For more information, refer to the **t1 linecode** controller configuration command in the *Cisco IOS Interface and Hardware Component Command Reference*.

Configuring External T1 Channels

The first three T1 channels (1, 2, and 3) of the CT3IP can be broken out to the DSUP-15 connectors so that the T1 channel can be further demultiplexed by the MIP on the same router, another router, or other multiplexing equipment.

Note If a T1 channel that was previously configured as a serial interface is broken out to the external T1 port, that interface and its associated configuration remain intact while the channel is broken out to the external T1 port. The serial interface is not usable during the time that the T1 channel is broken out to the external T1 port; however, the configuration remains to facilitate the return of the T1 channel to a serial interface using the **no t1 external** command.

To configure a T1 channel as an external port, use the following commands beginning in EXEC mode.

	Command	Purpose
Step 1	`Router# show controller t3 slot/port-adapter/port`	Displays the Ext1... field so that you can verify whether the external device connected to the external T1 port is configured and cabled correctly. If the line status is OK, a valid signal is being received and the signal is not an all-ones signal.
Step 2	`Router# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 3	Router(config)# **controller t3** *slot***/***port-adapter***/***port*	Selects the CT3IP and enters controller configuration mode.
Step 4	Router(config-controller)# **t1 external** *channel* [**cablelength** *feet*] [**linecode** {**ami** | **b8zs**}]	Configures the T1 channel (values are 1, 2, and 3) as an external port and optionally specifies the cable length and line code. Only T1 channels 1 through 3 can be configured as an external T1. The default **cablelength** is 133 feet, and the default **linecode** is **b8zs**. Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

After you configure the external T1 channel, you can continue configuring it as a channelized T1 from the MIP. All channelized T1 commands might not be applicable to the T1 interface. To define the T1 controller and enter controller configuration mode, use the following command in global configuration mode.

Command	Purpose
Router(config)# **controller t1** *slot***/***port*	Selects the MIP and enters controller configuration mode.

After you configure the channelized T1 on the MIP, you can continue configuring it as you would a normal serial interface. All serial interface commands might not be applicable to the T1 interface. To enter interface configuration mode and configure the serial interface that corresponds to a T1 channel group, use the following command in global configuration mode.

Command	Purpose
Router(config)# **interface serial** *slot***/***port***:***t1-channel*	Defines the serial interface for a T1 channel on the MIP (values are 1 to 28) and enters interface configuration mode.

For more information, see the "Configuring Each T1 Channel" section on page 256 and the "Specifying a Synchronous Serial Interface" section on page 236.

For an example of configuring an external T1 channel, see the "Channelized T3 Interface Processor Configuration Examples" section on page 303.

Monitoring and Maintaining the CT3IP

After configuring the new interface, you can monitor the status and maintain the CT3IP in the Cisco 7000 series routers with an RSP7000 or in the Cisco 7500 series routers by using the **show** commands. To display the status of any interface, use one of the following commands in EXEC mode.

Command	Purpose
`Router>` **`show controller cbus`**	Displays the internal status of each interface processor and lists each interface.
`Router>` **`show controller t3`** [*slot*/*port-adapter*/*port*[:*t1-channel*]] [**brief** | **tabular**]	Displays the status of the T3 and T1 channels (values are 1 to 28), including the T3 alarms and T1 alarms for all 28 T1 channels, or only the T1 channel specified.
`Router>` **`show interfaces serial`** *slot*/*port-adapter*/*port*:*t1-channel* [**accounting** | **crb**]	Displays statistics about the serial interface for the specified T1 channel (values are 1 to 28) on the router.

Verifying T3 Configuration

To verify your software configuration, you can use **show** commands for controller settings. To use **show** commands, you must be in privileged EXEC mode.

```
Router# show controller t3

T3 1/0/0 is up.
 Applique type is Channelized T3
 No alarms detected.
 FEAC code received: No code is being received
 Framing is M23, Line Code is B3ZS, Clock Source is Line.
 Data in current interval (751 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Total Data (last 16 15 minute intervals):
     0 Line Code Violations, 0 P-bit Coding Violation,
     0 C-bit Coding Violation, 0 P-bit Err Secs,
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
     0 Unavailable Secs, 0 Line Errored Secs,
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

Tip

- To use the controller, it must report being up.
- No errors should be reported.

Configuring Maintenance Data Link Messages

The CT3IP can be configured to send a Maintenance Data Link (MDL) message as defined in the ANSI T1.107a-1990 specification. To specify the transmission of the MDL messages, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)#` **`controllers t3`** *`slot`*`/`*`port-adapter`*`/`*`port`*	Selects the CT3IP and enters controller configuration mode.
Step 2	`Router(config-controller)#` **`mdl`** `{`**`transmit`** `{`**`path`** `|` **`idle-signal`** `|` **`test-signal`**`}` `|` **`string`** `{`**`eic`** `|` **`lic`** `|` **`fic`** `|` **`unit`** `|` **`pfi`** `|` **`port`** `|` **`generator`**`}` *`string`*`}`	Configures the MDL message.

Specify one **mdl** command for each message. For example, use **mdl string eic** *Router A* to transmit "Router A" as the equipment identification code and use **mdl string lic** *Test Network* to transmit "Test Network" as the location identification code.

Use the **show controllers t3** command to display MDL information (received strings). MDL information is displayed only when framing is set to C-bit.

Enabling Performance Report Monitoring

The CT3IP supports performance reports via the Facility Data Link (FDL) per ANSI T1.403. By default, performance reports are disabled. To enable FDL performance reports, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)#` **`controllers t3`** *`slot`*`/`*`port-adapter`*`/`*`port`*	Selects the CT3IP and enters controller configuration mode.
Step 2	`Router(config-controller)#` **`t1`** *`channel`* **`fdl ansi`**	Enables 1-second transmission of the performance report for a specific T1 channel (values are 1 to 28).

Note Performance reporting is available only on T1 channels configured for ESF framing.

To display the remote performance report information, use the following command in EXEC mode.

Command	Purpose
`Router>` **`show controllers t3`** `[`*`slot`*`/`*`port-adapter`*`/`*`port`*`[`**`:`***`t1-channel`*`]]` **`remote performance`** `[`**`brief`** `|` **`tabular`**`]`	Displays the remote performance report information for the T1 channel (values are 1 to 28).

Configuring for BERT on the Cisco AS5300

Bit-error rate testing (BERT) and loopbacks are used by carriers and Internet service providers (ISPs) to aid in problem resolution as well as testing the quality of T1/E1 links. BERT detects poor quality links early and isolates problems quickly, enabling Cisco AS5300 users to improve their quality of service and increase their revenues.

BERT is available for the Cisco AS5300 router for T1 and E1 facilities. Perform the following tasks to configure the Cisco AS5300 router for BERT, use the following commands beginning in user EXEC mode.

	Command	Purpose

Step 1	`5300>` **`enable`**
	`Password:` *`password`*
	`5300#`
		Enters privileged EXEC mode.

Step 2	`5300#` **`configure terminal`**	Enters global configuration mode.
Step 3	`Router(config)#` **`bert profile`**	Enables the user to configure up to 15 BERT profiles in addition to the default BERT profile 0, by using the extensions to this command.

Verifying BERT on the Cisco AS5300

To verify that a BERT feature is running, use the **show running-config** command in EXEC mode.

```
5300> show running-config
!
bert profile 1 pattern 1s threshold 10^-4 error-injection none duration 3
bert profile 7 pattern 220-O.151QRSS threshold 10^-3 error-injection 10^-5 duration 120
```

Enabling a BERT Test Pattern

To enable and disable generation of a BERT test pattern for a specified interval for a specific T1 channel, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)#` **`controller t3`** *`slot`***`/`***`port-adapter`***`/`***`port`*	Selects the CT3IP and enters controller configuration mode.
Step 2	`Router(config-controller)#` **`t1`** *`channel`* **`bert pattern`** `{`**`0s`** | **`1s`** | **`2^15`** | **`2^20`** | **`2^23`**`}` **`interval`** *`minutes`*	Enables a BERT test pattern on a T1 channel (values are 1 to 28).
Step 3	`Router(config-controller)#` **`no t1`** *`channel`* **`bert pattern`** `{`**`0s`** | **`1s`** | **`2^15`** | **`2^20`** | **`2^23`**`}` **`interval`** *`minutes`*	Disables a BERT test pattern on a T1 channel (values are 1 to 28).

The BERT test patterns from the CT3IP are framed test patterns (that is, the test patterns are inserted into the payload of the framed T1 signal).

To view the BERT results, use the **show controllers t3** or **show controllers t3 brief** EXEC command. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT test
- Total bit errors
- Total bits received

When the T1 channel has a BERT test running, the line state is DOWN. Also, when the BERT test is running and the Status field is Not Sync, the information in the total bit errors field is not valid. When the BERT test is done, the Status field is not relevant.

The **t1 bert pattern** command is not written to NVRAM because it is only used for testing the T1 channel for a short predefined interval and to avoid accidentally saving the command, which could cause the interface not to come up the next time the router reboots.

Enabling Remote FDL Loopbacks

You can perform the following types of remote Facility Data Link (FDL) loopbacks on a T1 channel:

- Remote payload FDL ANSI—Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback.
- Remote line FDL ANSI—Sends a repeating, 16-bit ESF data link code word (00001110 11111111) to the remote CSU end requesting that it enter into a network line loopback.
- Remote line FDL Bellcore—Sends a repeating, 16-bit ESF data link code word (00010010 11111111) to the remote SmartJack end requesting that it enter into a network line loopback.

To enable loopback on a T1 channel, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)#` **`interface serial`** *`slot`*`/`*`port-adapter`*`/`*`port`*`:`*`t1-channel`* (Cisco 7500 series and Cisco 7000 series routers with the RSP7000 and RSP7000CI) or `Router(config)#` **`interface serial`** *`slot`*`/`*`port`*`:`*`t1-channel`* (Cisco 7200 series)	Selects the T1 channel (values are 1 to 28) on the CT3IP and enters interface configuration mode.
Step 2	`Router(config-if)#` **`loopback remote payload`** `[`**`fdl`**`] [`**`ansi`**`]`	Enables the remote payload FDL ANSI bit loopback on the T1 channel.
Step 3	`Router(config-if)#` **`loopback remote line fdl`** `{`**`ansi`** `|` **`bellcore`**`}`	Enables the remote line FDL ANSI bit loopback or remote SmartJack loopback on the T1 channel.

Note The port adapter and port numbers for the CT3IP are 0.

Configuring T1 Cable Length and T1/E1 Line Termination

When you configure your channelized T1 trunk cards, you can change the line build-out of the cable pair connected to the port. To specify the build-out value, use either the **cablelength long** command or the **cablelength short** command. These commands are not required for E1 trunk cards.

For cables longer than 655 feet, use the **cablelength long** command; for cables up to and including 655 feet, use the **cablelength short** command.

The **line-termination** command allows you to set the T1/E1 port termination to 75 ohms unbalanced or 120 ohms balanced.

The following cable length short configurations define the length range (in feet) between your network access server (NAS) and your repeater. The **cablelength short** command is configured for a channelized T1 only and includes the following settings:

- 133 feet (0 to 133 feet)
- 266 feet (134 to 266 feet)
- 399 feet (267 to 399 feet)
- 533 feet (400 to 533 feet)
- 655 feet (534 to 655 feet)

Note Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes fixed configuration lengths. For example, if your cable length is 50 feet between your NAS and your repeater, you should configure your cable length using the 133-feet setting. If you later change the cable length to 200 feet, you should reconfigure your cable length using the 266-feet setting.

The following cable length long configurations define the length range in gain and pulse requirements for the length of build-out between your NAS and your repeater that is longer than 655 feet. The **cablelength long** command is configured for a channelized T1 only and includes the following gain and pulse settings:

- gain26 (26 dB gain)
- gain36 (36 dB gain)
- –15db (–15 dB pulse)
- –22.5db (–22.5 dB pulse)
- –7.5db (–7.5 dB pulse)
- 0db (0 dB pulse)

To configure channelized T1 lines for line build-out, use the following commands beginning in user EXEC mode.

	Command	Purpose
Step 1	Router> **enable** Password: *password* Router#	Enters privileged EXEC mode.
Step 2	Router# **configure terminal**	Enters global configuration mode. The example shown uses the terminal configuration option.
Step 3	Router(config)# **controller t1** *shelf***/***slot***/***port*	Enters controller configuration mode and specifies a shelf, slot, and port for the controller port. The controller ports are labeled *shelf***/***slot***/0** through *shelf***/***slot***/11** on the T1. (You must type in the slashes (/) as part of the command.

Step 4	Router(config-controller)# **cablelength short** {**133** | **266** | **399** | **533** | **655**}
	or
	Router(config-controller)# **cablelength long** {**gain26** | **gain36**} {**-15** | **-22.5** | **-7.5** | **0**}
		Specifies the controller **cablelength short** value between **0** and **655** (feet).
		Specifies the controller **cablelength long** value using **gain** and **pulse** settings for cables longer than 655 feet. (Configure cable length for T1 only.)

Step 5	Router(config-controller)# **line termination** {**75-ohm** | **120-ohm**}	Specifies the line-termination value. (The command is used for E1 only.)

Configuring PA-E3 and PA-2E3 Serial Port Adapters

The PA-E3 and PA-2E3 serial port adapters are available on:

- Cisco 7200 series routers
- Cisco 7500 series routers
- Cisco 7000 series routers with the 7000 series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI)

These port adapters provide one (PA-E3) or two (PA-2E3) high-speed, full-duplex, synchronous serial E3 interfaces and integrated data service unit (DSU) functionality.

The E3 port adapters can transmit and receive data at E3 rates of up to 34 Mbps and use a 75-ohm coaxial cable available from Cisco to connect to a serial E3 network. These port adapters support the following:

- 16- and 32-bit cyclic redundancy checks (CRCs)
- High-speed HDLC data
- G.751 framing or bypass
- HDB3 line coding
- ATM-DXI, Frame Relay, HDLC, PPP, and SMDS serial encapsulation
- National service bits
- E3 MIB (RFC 1407)
- Scrambling and reduced bandwidth
- Remote and local loopbacks

The PA-E3 port adapter supports the RFC 1407 DS3 Near End Group, including:

- DS3/E3 Configuration Table
- DS3/E3 Current Table
- DS3/E3 Interval Table
- DS3/E3 Total Table

The PA-E3 port adapter also supports the Card Table in the Cisco Chassis MIB and the MIB-2 for each PA-E3 interface.

The PA-E3 port adapter does not support the RFC 1407 DS3 Far End Group and DS3/E3 Fractional Group.

Note For additional information on the E3 serial port adapter, refer to the *PA-E3 Serial Port Adapter Installation and Configuration* publication.

PA-E3 and PA-2E3 Serial Port Adapter Configuration Task List

To configure the PA-E3, Perform the tasks in the following sections. Each task in the list is identified as either required or optional.

- Configuring the PA-E3 Port Adapter, page 266 (Required)
- Monitoring and Maintaining the PA-E3 Port Adapter, page 267 (Optional)

For PA-E3 port adapter configuration examples, see the "PA-E3 Serial Port Adapter Configuration Example" section on page 307.

Configuring the PA-E3 Port Adapter

The commands listed in Table 21 have been added to support the PA-E3 interface configuration. If you do not modify the configuration of the PA-E3, the configuration defaults shown in Table 21 are used.

Table 21 PA-E3 Port Adapter Defaults

Command	Default Value
dsu bandwidth	34,010 kbps
dsu mode	0
framing	g751
international bit	0 0
invert data	data is not inverted
national bit	0
scramble	disabled

If you need to change any of the default configuration attributes, use the first command in global configuration mode, followed by any of the optional commands in interface configuration mode.

Command	Purpose

`Router(config)# interface serial slot/port-adapter/port`
or
`Router(config)# interface serial slot/port`
	Selects the PA-E3 interface and enters interface configuration mode for the Cisco 7500 series and Cisco 7000 series routers with the RSP7000 and RSP7000CI.
	Selects the PA-E3 interface and enters interface configuration mode for the Cisco 7200 series.

`Router(config-if)# dsu bandwidth kbps`	Changes the DSU bandwidth.
`Router(config-if)# dsu mode {0 | 1}`	Changes the DSU mode. To connect to another PA-E3 port adapter or a Digital Link DSU, use the default mode (0). To connect to a Kentrox DSU, use mode 1.
`Router(config-if)# framing {g751 | bypass}`	Changes the framing used by the interface.
`Router(config-if)# international bit {0 | 1} {0 | 1}`	Changes the international bit used by the interface.
`Router(config-if)# invert data`	Inverts the data stream on the interface.
`Router(config-if)# national bit {0 | 1}`	Changes the national bit used by the interface.
`Router(config-if)# scramble`	Enables scrambling on the interface.

Monitoring and Maintaining the PA-E3 Port Adapter

After configuring the new interface, you can display its status. To show current status of the E3 interface on the PA-E3 port adapter, use any of the following commands in EXEC mode.

Command	Purpose

`Router> show interfaces serial slot/port-adapter/port`
or
`Router> show interfaces serial slot/port`
	Displays statistics for the E3 interface for the Cisco 7500 series and Cisco 7000 series routers with the RSP7000 and RSP7000CI.
	Displays statistics for the E3 interface for the Cisco 7200 series.

`Router> show controllers serial slot/port-adapter/port`
or
`Router> show controllers serial slot/port`
	Displays the configuration information for the E3 interface for the Cisco 7500 series and Cisco 7000 series routers with the RSP7000 and RSP7000CI
	Displays the configuration information for the E3 interface for the Cisco 7200 series.

Configuring PA-T3 and PA-2T3 Serial Port Adapters

The PA-T3 and PA-2T3 serial port adapters are available on:

- Cisco 7200 series routers
- Second-generation Versatile Interface Processor (VIP2) in all Cisco 7500 series routers
- Cisco 7000 series routers with the 7000 series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI)

These port adapters provide one (PA-T3) or two (PA-2T3) high-speed, full-duplex, synchronous serial T3 interfaces and integrated data service unit (DSU) functionality.

The T3 port adapters can transmit and receive data at T3 rates of up to 45 Mbps and use a 75-ohm coaxial cable available from Cisco to connect to a serial T3 network. These port adapters support the following features:

- 16- and 32-bit cyclic redundancy checks (CRCs)
- High-speed HDLC data
- C-bit, M13, and bypass framing
- HDB3 line coding
- ATM-DXI, Frame Relay, HDLC, PPP, and SMDS serial encapsulation
- DS3 MIB (RFC 1407)
- Scrambling and reduced bandwidth
- Remote and local loopbacks

Note For additional information on interoperability guidelines for T3 serial port adapter DSUs, refer to the *PA-T3 Serial Port Adapter Installation and Configuration* publication.

PA-T3 and PA-2T3 Port Adapter Configuration Task List

To configure the PA-T3 port adapters, perform the tasks in the following sections. Each task is identified as either required or optional.

- Configuring the PA-T3 Port Adapter, page 268 (Required)
- Troubleshooting the PA-T3 Port Adapter, page 269 (Optional)
- Monitoring and Maintaining the PA-T3 Port Adapter, page 270 (Optional)

For PA-T3 port adapter configuration examples, see the “PA-T3 and PA-2T3 Configuration Example” section on page 307.

Configuring the PA-T3 Port Adapter

The commands listed in Table 22 have been added to support the PA-T3 interface configuration. If you do not modify the configuration of the PA-T3, the configuration defaults shown in Table 22 are used.

Table 22 PA-T3 Port Adapter Defaults

Command	Default Value
cablelength	49
clock source	line
crc 32	16-bit
dsu bandwidth	44,736 kbps
dsu mode	0
framing	C-bit
invert data	data is not inverted
scramble	disabled

If you need to change any of the default configuration attributes, use the first command in global configuration mode, followed by any of the optional commands in interface configuration mode.

Command	Purpose
`Router(config)#` **interface serial** *slot***/***port-adapter***/***port* or `Router(config)#` **interface serial** *slot***/***port*	Selects the PA-T3 interface and enters interface configuration mode for the Cisco 7500 series and Cisco 7000 series routers with the RSP7000 and RSP7000CI. Selects the PA-T3 interface and enters interface configuration mode for the Cisco 7200 series.
`Router(config-if)#` **cablelength** *length*	Changes the cable length.
`Router(config-if)#` **crc 32**	Enables 32-bit CRC.
`Router(config-if)#` **dsu bandwidth** *kbps*	Changes the DSU bandwidth.
`Router(config-if)#` **dsu mode** {**0** | **1** | **2**}	Changes the DSU mode. To connect to another PA-T3 port adapter or a Digital Link DSU, use the default mode (0). To connect to a Kentrox DSU, use mode 1. To connect to a Larscom DSU, use mode 2.
`Router(config-if)#` **framing** {**c-bit** | **m13** | **bypass**}	Changes the framing used by the interface.
`Router(config-if)#` **invert data**	Inverts the data stream on the interface.
`Router(config-if)#` **scramble**	Enables scrambling on the interface.

Troubleshooting the PA-T3 Port Adapter

To set the following loopback modes to troubleshoot the PA-T3 port adapter using Cisco IOS software, use the first command in global configuration mode, followed by any of the other commands depending on your needs:

Command	Purpose
`Router(config)#` **loopback dte**	Loops back after the LIU toward the terminal.
`Router(config)#` **loopback local**	Loops back after going through the framer toward the terminal.

Command	Purpose
Router(config)# **loopback network line**	Loops back toward the network before going through the framer.
Router(config)# **loopback network payload**	Loops back toward the network after going through the framer.
Router(config)# **loopback remote**	Sends a far-end alarm control (FEAC) to set the remote framer in loopback.

These loopback commands loop all packets from the T3 interface back to the interface or direct packets from the network back out toward the network.

Monitoring and Maintaining the PA-T3 Port Adapter

After configuring the new interface, you can display its status. To show current status of the T3 interface on the PA-T3 port adapter, use any of the following commands in EXEC mode.

Command	Purpose
Router> **show version**	Displays system hardware configuration.
Router> **show controllers cbus**	Displays current interface processors and their interfaces.
Router> **show interfaces** *slot***/***port-adapter***/***port* (Cisco 7500 series and Cisco 7000 series routers with the RSP7000 and RSP7000CI) Router> **show interfaces** *slot***/***port* (Cisco 7200 series)	Displays statistics for the T3 interface.
Router> **show controllers serial** *slot***/***port-adapter***/***port* (Cisco 7500 series and Cisco 7000 series routers with the RSP7000 and RSP7000CI) Router> **show controllers serial** *slot***/***port* (Cisco 7200 series)	Displays the configuration information for the T3 interface.
Router> **show protocols**	Displays protocols configured for the system and specific interfaces.
Router> **more system:running-config**	Displays the running configuration file.
Router> **more nvram:startup-config**	Displays the configuration stored in NVRAM.
Router> **show diag** *slot*	Displays specific port adapter information

Configuring a Packet OC-3 Interface

The Cisco Packet OC-3 Interface Processor (POSIP) and Packet OC-3 Port Adapter (POSPA) are available on:

- Cisco 7500 series routers
- Cisco 7200 series routers

The Packet-Over-SONET OC-3 port adapters (PA-POS-OC3SML, PA-POS-OC3SMI, and PA-POS-OC3MM) are available on:

- Cisco 7500 series routers
- Cisco 7200 series routers
- Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI)

The POSIP and POS OC-3 provide a single 155.520-Mbps, OC-3 physical layer interface for packet-based traffic. This OC-3 interface is fully compatible with SONET and Synchronous Digital Hierarchy (SDH) network facilities and is compliant with RFC 1619, "PPP over SONET/SDH," and RFC 1662, *PPP in HDLC-like Framing*. The Packet-Over-SONET specification is primarily concerned with the use of PPP encapsulation over SONET/SDH links.

For more information on the PA-POS-OC3 port adapter, refer to the *PA-POS-OC3 Packet OC-3 Port Adapter Installation and Configuration* publication that accompanies the hardware.

The POS is a fixed-configuration interface processor that uses second-generation Versatile Interface Processor (VIP2) technology. The POS provides a single 155.520-Mbps, OC-3 physical layer interface for packet-based traffic. This OC-3 interface is fully compatible with SONET and SDH network facilities and is compliant with RFC 1619 and RFC 1662. The Packet-Over-SONET specification primarily addresses the use of PPP encapsulation over SONET/SDH links.

Table 23 describes the default values set in the initial configuration of a Packet OC-3 interface.

Table 23 Packet OC-3 Interface Default Configuration

Attributes	Default Value
Maximum transmission unit (MTU)	4470 bytes
Framing	SONET STS-3c framing
Loopback internal	No internal loopback
Loopback line	No line loopback
Transmit clocking	Recovered receive clock
Enabling	Shut down

Because the Packet OC-3 interface is partially configured, you might not need to change its configuration before enabling it. However, when the router is powered up, a new Packet OC-3 interface is shut down. To enable the Packet OC-3 interface, you must use the **no shutdown** command in the global configuration mode.

Packet OC-3 Interface Configuration Task List

The values of all Packet OC-3 configuration parameters can be changed to match your network environment. To customize the POS configuration, perform the tasks in the following sections. Each task in the list is identified as either required or optional.

- Selecting a Packet OC-3 Interface, page 272 (Optional)
- Setting the MTU Size, page 272 (Optional)
- Configuring Framing, page 273 (Optional)
- Configuring an Interface for Internal Loopback, page 273 (Optional)

- Configuring an Interface for Line Loopback, page 273 (Optional)
- Setting the Source of the Transmit Clock, page 274 (Optional)
- Enabling Payload Scrambling, page 274 (Optional)
- Configuring an Alarm Indication Signal, page 274 (Optional)

Selecting a Packet OC-3 Interface

The Packet OC-3 interface is referred to as *pos* in the configuration commands. An interface is created for each POS found in the system at reset time.

If you need to change any of the default configuration attributes or otherwise reconfigure the Packet OC-3 interface, use one the following commands in global configuration mode.

Command	Purpose

`Router(config)# interface pos slot/port`
(Cisco 7200)
or
`Router(config)# interface pos slot/port-adapter/port`
(Cisco 7500)
	Selects the Packet OC-3 interface and enters interface configuration mode.

Setting the MTU Size

To set the maximum transmission unit (MTU) size for the interface, use the following command in interface configuration mode.

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

The value of the *bytes* argument is in the range 64 to 4470 bytes; the default is 4470 bytes (4470 bytes exactly matches FDDI and HSSI interfaces for autonomous switching). The **no** form of the command restores the default.

Caution Changing an MTU size on a Cisco 7500 series router will result in resizing and reassignment of buffers and resetting of all interfaces. The following message is displayed:

```
%RSP-3-Restart:cbus complex88
```

Configuring Framing

To configure framing on the Packet OC-3 interface, use one of the following commands in interface configuration mode.

Command	Purpose
`Router(config-if)# pos framing-sdh`	Selects SDH STM-1 framing.
`Router(config-if)# no pos framing-sdh`	Reverts to the default SONET STS-3c framing.

Configuring an Interface for Internal Loopback

With the **loopback internal** command, packets from the router are looped back in the framer. Outgoing data gets looped back to the receiver without actually being transmitted. With the **loopback line** command, the receive fiber (RX) is logically connected to the transmit fiber (TX) so that packets from the remote router are looped back to it. Incoming data gets looped around and retransmitted without actually being received.

To enable or disable internal loopback on the interface, use one of the following commands in interface configuration mode.

Command	Purpose
`Router(config-if)# loop internal`	Enables internal loopback.
`Router(config-if)# no loop internal`	Disables internal loopback.

Local loopback is useful for checking that the POS is working. Packets from the router are looped back in the framer.

Configuring an Interface for Line Loopback

Line loopback is used primarily for debugging purposes.

To enable or disable an interface for line loopback, use one of the following commands in interface configuration mode.

Command	Purpose
`Router(config-if)# loop line`	Enables line loopback.
`Router(config-if)# no loop line`	Disables line loopback.

The receive fiber (RX) is logically connected to the transmit fiber (TX) so that packets from the remote router are looped back to it.

Setting the Source of the Transmit Clock

By default, the Packet OC-3 interface uses the recovered receive clock to provide transmit clocking. To change the transmit clock source, use one of the following commands in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`clock source`**	Sets the internal clock as the transmit clock source.
`Router(config-if)#` **`no clock source`**	Sets the recovered receive clock to provide transmit clocking.

Enabling Payload Scrambling

SONET payload scrambling applies a self-synchronous scrambler (x^{43}+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density. Both ends of the connection must use the same scrambling algorithm. When enabling POS scrambling on a VIP2 POS on the Cisco 7500 series router that has a hardware revision of 1.5 or higher, you can specify CRC 16 only (that is, CRC 32 is currently not supported).

To enable SONET payload scrambling on a POS interface, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`pos scramble-atm`**	Enables SONET payload scrambling.

Configuring an Alarm Indication Signal

To configure line alarm indication signals (LAIS) when the POS interface is placed in any administrative shut down state, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)#` **`pos ais-shut`**	Sends line alarm indication signals.

Configuring a DPT OC-12c Interface

The dual-width OC-12c Dynamic Packet Transport (DPT) port adapter is available on Cisco 7200 series routers and Cisco 7200 VXR series routers with the correct Route Switch Processor (RSP2 or RSP4), running Cisco IOS Release 12.0(6)S or later, to provide shared IP-over-SONET capability.

The OC-12c Dynamic Packet Transport Interface Processor (DPTIP) is available on Cisco 7500 series routers with the correct Route Switch Processor (RSP2 or RSP4), running Cisco IOS Release 12.0(6)S or later. The DPT is an OC-12c interface that uses second-generation Versatile Interface Processor (VIP2) technology to provide shared IP-over-SONET capability, and it complies with IEEE 802.3 specifications for multicast and broadcast media. The DPTIP assembly consists of a VIP2 with a dual-width DPT interface processor permanently attached to it.

The DPT interface provides the following benefits:

- Accommodates large-scale network topology.
- Complies with applicable IEEE 802.3 standards.
- Supports Intelligent Protection Switching (IPS).

OC-12c Interface Configuration Task List

To configure the DPT interface, perform the tasks in the following sections. Each task in the list is identified as either required or optional.

- Configuring the Dynamic Packet Transport Interface, page 275 (Required)
- Configuring Intelligent Protection Switching, page 276 (Optional)
- Configuring DPT Topology, page 276 (Optional)

Configuring the Dynamic Packet Transport Interface

	Command or Action	Purpose
Step 1	`Router# show running-config`	Confirms that the system recognizes the DPT or DTPIP.
Step 2	`Router# configure terminal`	Enters configuration mode.
Step 3	`Router(config)# ip routing`	Enables IP routing.

Step 4	`Router(config)# interface srp slot/port`
	(Cisco 7200 series router)
	`Router(config)# interface srp slot/port-adapter/port`
	(Cisco 7500 series router)
		Specifies an interface.
		The interface type of the DPT or DPTIP is Spatial Reuse Protocol (SRP).

Step 5	`Router(config-if)# ip address 192.168.2.3 255.255.255.0`	Assigns an IP address and subnet mask to the interface.
Step 6	Add any additional configuration commands required to enable routing protocols, and set the interface characteristics for your configuration requirements.	
Step 7	`Router(config-if)# no shutdown`	Changes the shutdown state to up and enables the interface.
Step 8	`Router(config-if)# Ctrl-Z`	Includes all the configuration commands to complete the configuration and exits interface configuration mode.
Step 9	`Router# copy running-config startup-config`	Writes the new configuration to the startup configuration.

The system displays an OK message when the configuration has been stored.

Use the **show running-config** command to verify the currently running configuration. Use the **show version** command to display the configuration of the system hardware and the Cisco IOS software information.

Configuring Intelligent Protection Switching

The SRP interface uses ring architecture to provide redundancy and protection from a failed node or a fiber cut by using Intelligent Protection Switching (IPS). To configure IPS, use the following commands beginning in privileged EXEC mode. The steps described in this section are optional.

	Command	Purpose
Step 1	`Router# configure terminal`	Enables configuration mode.

Step 2	`Router(config)# interface srp slot/port`
	(Cisco 7200 series routers)
	`Router(config)# interface srp slot/port-adapter/port`
	(Cisco 7500 series routers)
		Configures an SRP interface.

Step 3	`Router(config-if)# srp ips request manual-switch a`	Specifies an IPS manual switch on side A or side B.
Step 4	`Router(config-if)# srp ips wtr-timer 10`	Specifies a wait-to-restore request (in seconds) to prevent switch oscillations on side A.
Step 5	`Router(config-if)# srp ips timer 20 a`	Configures a message timer to be sent to the inner and outer rings to control the frequency of IPS message transmissions on side A.
Step 6	`Router(config-if)# ^Z`	Exits configuration mode.

Use the **show srp** command to verify the configuration.

Configuring DPT Topology

Every node on a DPT ring maintains a topology map of the ring, so that it knows where to route traffic. It updates the topology map by periodically sending a query, called a topology discovery packet, out onto the outer-ring path. Each node on the ring adds its own MAC address to the packet. When the discovery packet returns to the originating node, the contents of the packet are used to update the topology map. You use the **srp topology-timer** command to set the frequency with which the node sends out topology discovery packets. To configure DPT, use the following commands beginning in privileged EXEC mode.

	Command	Purpose
Step 1	`Router# configure terminal`	Enables interface configuration mode.

Step 2	`Router(config)# interface srp slot/port`
	(Cisco 7200 series routers)
	`Router(config)# interface srp slot/port-adapter/port`
	(Cisco 7500 series routers)
		Configures an SRP interface.

Step 3	`Router(config-if)# srp topology-timer 70`	Configures the frequency of the topology message timer in seconds.
Step 4	`Router(config-if)# ^Z`	Exits configuration mode.
Step 5	`Router# show srp topology`	Confirms the identity of the nodes on the ring; shows the number of hops between nodes; identifies the nodes that are in wrap mode. Use the **show srp topology** command to show the identity of the nodes on the DPT ring according to their MAC addresses.

Configuring Automatic Protection Switching of Packet-over-SONET Circuits

The automatic protection switching (APS) feature is supported on Cisco 7500 series routers. This feature allows switchover of Packet-over-SONET (POS) circuits and is often required when connecting SONET equipment to telco equipment. APS refers to the mechanism of bringing a “protect” POS interface into the SONET network as the “working” POS interface on a circuit from the intervening SONET equipment.

The protection mechanism used for this feature is “1+1, Bidirectional, nonrevertive” as described in the Bellcore publication “TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, Section 5.3.” In the 1+1 architecture, there is one working interface (circuit) and one protect interface, and the same payload from the transmitting end is sent to both the receiving ends. The receiving end decides which interface to use. The line overhead (LOH) bytes (K1 and K2) in the SONET frame indicate both status and action.

The protect interface is configured with the IP address of the router that has the working interface. The APS Protect Group Protocol, which runs on top of UDP, provides communication between the process controlling the working interface and the process controlling the protect interface. Using this protocol, POS interfaces can be switched because of a router failure, degradation or loss of channel signal, or manual intervention. In bidirectional mode, the receive and transmit channels are switched as a pair. In unidirectional mode, the transmit and receive channels are switched independently. For example, if the receive channel on the working interface has a loss of channel signal, both the receive and transmit channels are switched.

In addition to the new Cisco IOS commands added for the APS feature, the POS interface configuration commands **pos threshold** and **pos report** have been added to support user configuration of the bit-error rate (BER) thresholds and reporting of SONET alarms.

APS Configuration Task List

Two SONET connections are required to support APS. In a telco environment, the SONET circuits must be provisioned as APS. You must also provision the operation (for example, 1+1), mode (for example, bidirectional), and revert options (for example, no revert). If the SONET connections are homed on two separate routers (the normal configuration), an out of band (OOB) communications channel between the two routers needs to be set up for APS communication.

When configuring APS, we recommend that you configure the working interface first. Normal operation with 1+1 operation is to configure it as a working interface. Also configure the IP address of the interface being used as the APS OOB communications path.

For more information on POS interfaces, refer to the installation and configuration documentation that accompanies the POS hardware.

To configure APS and POS, perform the following tasks. Each task is identified as either required or optional.

- Configuring APS Working and Protect Interfaces, page 278 (Required)
- Configuring Other APS Options, page 278 (Optional)
- Monitoring and Maintaining APS, page 279 (Optional)
- Configuring SONET Alarm Reporting, page 279 (Optional)
- Configuring a Protection Switch, page 280 (Optional)

Configuring APS Working and Protect Interfaces

This section describes how to configure and protect a working interface. The commands listed in this section are required. To avoid having the protected interface become the active circuit and disabling the working circuit when it is discovered, configure the working interface before configuring the protected interface.

To configure the working interface, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)# interface pos slot/port-adapter/port`	Specifies the POS interface to be configured as the working interface and enters interface configuration mode.
Step 2	`Router(config-if)# aps working circuit-number`	Configures this interface as a working interface.
Step 3	`Router(config-if)# end`	Exits configuration mode.

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

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

To configure the protect interface, use the following commands beginning in global configuration mode.

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

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

Configuring Other APS Options

To configure the other APS options, use any of the following optional commands in interface configuration mode.

Command	Purpose
`Router(config-if)# aps authenticate string`	(Optional) Enables authentication and specifies the string that must be present to accept any packet on the OOB communication channel.
`Router(config-if)# aps force circuit-number`	(Optional) Manually switches the specified circuit to a protect interface, unless a request of equal or higher priority is in effect.

Command	Purpose
`Router(config-if)#` **`aps group`** *`group-number`*	(Optional) Allows more than one protect/working interface group to be supported on a router.
`Router(config-if)#` **`aps lockout`** *`circuit-number`*	(Optional) Prevents a working interface from switching to a protect interface.
`Router(config-if)#` **`aps manual`** *`circuit-number`*	(Optional) Manually switches a circuit to a protect interface, unless a request of equal or higher priority is in effect.
`Router(config-if)#` **`aps revert`** *`minutes`*	(Optional) Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
`Router(config-if)#` **`aps timers`** *`seconds1 seconds2`*	(Optional) Changes the time between hello packets and the time before the protect interface process declares a working interface's router to be down (that is, seconds1 for the hello time and seconds2 for the hold time).
`Router(config-if)#` **`aps unidirectional`**	(Optional) Configures a protect interface for unidirectional mode.

Monitoring and Maintaining APS

To provide information about system processes, the Cisco IOS software includes an extensive list of EXEC commands that begin with the word **show**, which, when executed, display detailed tables of system information. Following is a list of some of the common **show** commands for the APS feature.

To display the information described, use these commands in privileged EXEC mode.

Command	Purpose
`Router#` **`show aps`**	Displays information about the automatic protection switching feature.
`Router#` **`show controllers pos`**	Displays information about the hardware.
`Router#` **`show interfaces pos`**	Displays information about the interface.

Configuring SONET Alarm Reporting

To configure the thresholds and the type of SONET alarms that are reported, use any of the following commands in interface configuration mode. The commands listed in this section are optional. The default settings are adequate for most POS installations.

Command	Purpose
`Router(config-if)#` **`pos threshold`** `{`**`b1-tca`** `|` **`b2-tca`** `|` **`b3-tca`** `|` **`sd-ber`** `|` **`sf-ber`**`}` *`rate`*	(Optional) Configures the BER threshold values for signal failure (SF), signal degrade (SD), or threshold crossing alarms (TCAs).
`Router(config-if)#` **`pos report`** `{`**`b1-tca`** `|` **`b2-tca`** `|` **`b3-tca`** `|` **`lais`** `|` **`lrdi`** `|` **`pais`** `|` **`plop`** `|` **`prdi`** `|` **`rdool`** `|` **`sd-ber`** `|` **`sf-ber`** `|` **`slof`** `|` **`slos`**`}`	(Optional) Enables reporting of selected SONET alarms.

To display the current BER threshold setting or to view the reporting of the SONET alarms, use the **show controllers pos** EXEC command.

Configuring a Protection Switch

LAIS can be used to force a protection switch in an APS environment. To force an APS switch when the interface is placed in administrative shut down state, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# pos ais-shut`	Sends line alarm indication signals.

Configuring Serial Interfaces for CSU/DSU Service Modules

The Cisco T1 data service unit/channel service unit (DSU/CSU) WAN interface card is an integrated, managed T1 or fractional T1 WAN interface card. It provides nonchannelized data rates of 1 to 24 X 64 kbps or 1 to 24 X 56 kbps and follows ANSI T1.403 and AT&T Publication 62411 standards.

The Cisco DSU/CSU WAN T1 interface includes the following management features:

- You can remotely configure the interface using Telnet and the Cisco IOS command-line interface (CLI).
- For monitoring purposes, the router and DSU/CSU are manageable as a single Simple Network Management Protocol (SNMP) entity using CiscoWorks or CiscoView. DSU/CSU statistics are accessed from the CLI.
- The SNMP agent supports the standard MIB II, Cisco integrated DSU/CSU MIB, and T1 MIB (RFC 1406).
- Loopbacks (including a manual button for a network line loopback) and bit error rate tester (BERT) tests are provided for troubleshooting.
- Test patterns, alarm counters, and performance reports are accessible using the CLI.
- The module has carrier detect, loopback, and alarm LEDs.

The following CSU and DSU service modules are described in this section:

- Fractional T1/FT/WIC CSU/DSU service module
- 2-wire and 4-wire, 56/64-kbps CSU/DSU service module

Fractional T1/FT/WIC CSU/DSU Service Module Configuration Task List

To configure fractional T1 and T1 (FT1/T1) service modules, perform the tasks described in these sections. Each task in the list is identified as either required or optional.

- Specifying the Clock Source, page 281 (Required)
- Enabling Data Inversion Before Transmission, page 281 (Required)
- Specifying the Frame Type of an FT/T1 Line, page 282 (Required)
- Specifying the CSU Line Build-Out, page 282 (Required)
- Specifying FT1/T1 Line-Code Type, page 282 (Required)
- Enabling Remote Alarms, page 283 (Optional)

- Enabling Loop Codes That Initiate Remote Loopbacks, page 283 (Optional)
- Specifying Time Slots, page 284 (Required)
- Enabling the T1 CSU WIC, page 284 (Required)

Specifying the Clock Source

To specify the clock source (that is, the source of the timing synchronization signal) for the FT1/T1 CSU/DSU module, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# service-module t1 clock source {internal | line}`	Specifies the clock source, for the CSU/DSU internal clock or the line clock.

Enabling Data Inversion Before Transmission

Data inversion is used to guarantee the ones density requirement on an alternate mark inversion (AMI) line when using bit-oriented protocols such as High-Level Data Link Control (HDLC), PPP, X.25, and Frame Relay.

To guarantee the ones density requirement on an AMI line using the FT1/T1 CSU/DSU module, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# service-module t1 data-coding inverted`	Inverts bit codes by changing all 1 bits to 0 bits and all 0 bits to 1 bits.

If the time-slot speed is set to 56 kbps, this command is rejected because line density is guaranteed when transmitting at 56 kbps. Use this command with the 64-kbps line speed. If you transmit inverted bit codes, both CSU/DSUs must have this command configured for successful communication.

To enable normal data transmission on an FT1/T1 network, use the following command in interface configuration mode.

Command	Purpose

`Router(config-if)# service-module tx1 data-coding normal`
or
`Router(config-if)# no service-module t1 data-coding inverted`
	Enables normal data transmission on a T1 network.

Specifying the Frame Type of an FT/T1 Line

To specify the frame type for a line using the FT1/T1 CSU/DSU module, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# service-module t1 framing {sf	esf}`	Specifies a FT1/T1 frame type. Choose either D4 Super Frame (**sf**) or Extended Super Frame (**esf**).

In most cases, the service provider determines which framing type, either **sf** or e**sf**, is required for your circuit.

Specifying the CSU Line Build-Out

To decrease the outgoing signal strength to an optimum value for the telecommunication carrier network, use the following command on the FT1/T1 CSU/DSU module in interface configuration mode.

Command	Purpose
`Router(config-if)# service-module t1 lbo {-15 db	-7.5 db}`	Decreases the outgoing signal strength in decibels.

To transmit packets without decreasing outgoing signal strength, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# service-module t1 lbo none`	Transmits packets without decreasing outgoing signal strength.

The ideal signal strength should be between –15 dB and –22 dB, which is calculated by adding the phone company loss plus cable length loss plus line build out. You may use this command in back-to-back configurations, but it is not needed on most actual T1 lines.

Specifying FT1/T1 Line-Code Type

To configure the line code for the FT1/T1 CSU/DSU module, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# service-module t1 linecode {ami	b8zs}`	Specifies a line-code type. Choose alternate mark inversion (AMI) or binary 8 zero substitution (B8ZS).

Configuring B8ZS is a method of ensuring the ones density requirement on a T1 line by substituting intentional bipolar violations in bit positions four and seven for a sequence of eight zero bits. When you configure the CSU/DSU AMI, you must guarantee the ones density requirement in your router using the

service-module t1 data-coding inverted command or the **service-module t1 timeslots speed 56** command. In most cases, your T1 service provider determines which line-code type, either **ami** or **b8zs**, is required for your T1 circuit.

Enabling Remote Alarms

To generate remote alarms (yellow alarms) at the local CSU/DSU or to detect remote alarms sent from the remote CSU/DSU, use the following command in interface configuration mode.

Command	Purpose
Router(config-if)# **service-module t1 remote-alarm-enable**	Enables remote alarms.

Remote alarms are transmitted by the CSU/DSU when it detects an alarm condition, such as a red alarm (loss of signal) or blue alarm (unframed 1s). The receiving CSU/DSU then knows that there is an error condition on the line.

With D4 Superframe configured, a remote alarm condition is transmitted by setting the bit 2 of each time slot to zero. For received user data that has bit 2 of each time slot set to zero, the CSU/DSU interprets the data as a remote alarm and interrupts data transmission, which explains why remote alarms are disabled by default. With Extended Super Frame configured, the remote alarm condition is signalled out of band in the facility data link.

You can see if the FT1/T1 CSU/DSU is receiving a remote alarm (yellow alarm) by issuing the **show service-module** command.

To disable remote alarms, use the following command in interface configuration mode.

Command	Purpose
Router(config-if)# **no service-module t1 remote-alarm-enable**	Disables remote alarms.

Enabling Loop Codes That Initiate Remote Loopbacks

To specify if the fractional T1/T1 CSU/DSU module goes into loopback when it receives a loopback code on the line, use the following commands in interface configuration mode.

	Command	Purpose
Step 1	Router(config-if)# **service-module t1 remote-loopback full**	Configures the remote loopback code used to transmit or accept CSU loopback requests.
Step 2	Router(config-if)# **service-module t1 remote-loopback payload** [**alternate** | **v54**]	Configures the loopback code used by the local CSU/DSU to generate or detect payload-loopback commands.

Note By using the **service-module t1 remote-loopback** command without specifying any keywords, you enable the standard-loopup codes, which use a 1-in-5 pattern for loopup and a 1-in-3 pattern for loopdown.

You can simultaneously configure the **full** and **payload** loopback points. However, only one loopback payload code can be configured at a time. For example, if you configure the **service-module t1 remote-loopback payload alternate** command, a payload v.54 request, which is the industry standard and default, cannot be transmitted or accepted. Full and payload loopbacks with standard-loopup codes are enabled by default.

The **no** form of this command disables loopback requests. For example, the **no service-module t1 remote-loopback full** command ignores all full-bandwidth loopback transmissions and requests. Configuring the **no** form of the command may not prevent telco line providers from looping your router in **esf** mode, because fractional T1/T1 telcos use facilities data-link messages to initiate loopbacks.

If you enable the **service-module t1 remote-loopback** command, the **loopback remote** commands on the FT1/T1 CSU/DSU module will not be successful.

Specifying Time Slots

To define time slots for an FT1/T1 module, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# service-module t1 timeslots {range | all} [speed {56 | 64}]`	Specifies time slots.

This command specifies which time slots are used in fractional T1 operation and determines the amount of bandwidth available to the router in each time slot. The *range* specifies the DS0 time slots that constitute the FT1/T1 channel. The range is from 1 to 24, where the first time slot is numbered 1, and the last time slot is numbered 24. Specify this field by using a series of subranges separated by commas. The time-slot range must match the time slots assigned to the channel group. In most cases, the service provider defines the time slots that comprise a channel group. Use the **no** form of this command to select all FT1/T1 time slots that are transmitting at 64 kbps, which is the default.

To use the entire T1 line, enable the **service-module t1 timeslots all** command.

Enabling the T1 CSU WIC

The following are prerequisites to enable the T1 CSU WIC:

- Leased line from your telephone company
- Configuration parameters depending on your specific telephone company. For most connections, the default settings should suffice:
  - **service-module t1 clock source line**
  - **service-module t1 data-coding normal**
  - **service-module t1 timeslots all speed 64**
  - **service-module t1 framing esf**
  - **service-module t1 lbo none**
  - **service-module t1 linecode b8zs**
  - **no service-module t1 remote-alarm-enable**
  - **no service-module t1 fdl**

Note To view the current configuration, use the **show service-module serial** *slot/port* command. For further information about these commands and how to change them, refer to the Cisco IOS configuration guides and command references that shipped with your router.

To configure the router to send SNMP traps, use the following commands:

	Command	Purpose
Step 1	`Router(config)#` **`interface serial`** *`slot/port`*	Enters interface configuration mode. The *slot/port* argument corresponds to where the WAN interface card is installed in your router.
Step 2	`Router(config-if)#` **`service-module t1 fdl`** `{`**`ansi`** `|` **`att`**`}`	Sets the **fdl** parameter to either **ansi** or **att**.
Step 3	`Router(config-if)#` **`Ctrl-Z`**	Exits interface configuration mode.
Step 4	`Router(config)#` **`more system:running-config`**	Displays the **fdl** parameter so that you can verify that it has changed.

2-Wire and 4-Wire, 56/64-kbps CSU/DSU Service Module Configuration Task List

To configure 2- and 4-wire, 56/64 kbps service modules, perform the tasks described in these sections:

- Setting the Clock Source, page 285
- Setting the Network Line Speed, page 286
- Enabling Scrambled Data Coding, page 286
- Changing Between Digital Data Service and Switched Dial-Up Modes, page 287
- Enabling Acceptance of a Remote Loopback Request, page 287
- Selecting a Service Provider, page 288

Setting the Clock Source

In most applications, the CSU/DSU should be configured using the **service-module 56k clock source line** command. For back-to-back configurations, use the **internal** keyword to configure one CSU/DSU and use the **line** keyword to configure the other CSU/DSU.

To configure the clock source for a 4-wire, 56/64-kbps CSU/DSU module, use the following command in interface configuration mode for a serial interface:

Command	Purpose
`Router(config-if)#` **`service-module 56k clock source`** `{`**`line`** `|` **`internal`**`}`	Configures the clock source.

Use the **no** form of this command to revert to the default clock source, which is the line clock.

Setting the Network Line Speed

To configure the network line speed for a 4-wire, 56/64-kbps CSU/DSU module, use the following command in interface configuration mode for a serial interface:

Command	Purpose
`Router(config-if)# service-module 56k clock rate speed`	Sets the network line speed.

You can use the following line speed settings: 2.4, 4.8, 9.6, 19.2, 38.4, 56, 64 kbps, and an **auto** setting.

The 64-kbps line speed cannot be used with back-to-back digital data service (DDS) lines. The subrate line speeds are determined by the service provider.

Only the 56-kbps line speed is available in switched mode. Switched mode is the default on the 2-wire CSU/DSU and is enabled by the **service-module 56k network-type** interface configuration command on the 4-wire CSU/DSU.

The **auto** linespeed setting enables the CSU/DSU to decipher current line speed from the sealing current running on the network. Because back-to-back DDS lines do not have sealing current, use the **auto** setting only when transmitting over telco DDS lines and using the line clock as the clock source.

Use the **no** form of this command to enable a network line speed of 56 kbps, which is the default.

Enabling Scrambled Data Coding

To prevent application data from replicating loopback codes when operating at 64 kbps on a 4-wire CSU/DSU, use the following command in interface configuration mode for a serial interface:

Command	Purpose
`Router(config-if)# service-module 56k data-coding scrambled`	Scrambles bit codes before transmission.

Enable the scrambled configuration only in 64 kbps DDS mode. If the network type is set to switched, the configuration is refused.

If you transmit scrambled bit codes, both CSU/DSUs must have this command configured for successful communication.

To enable normal data transmission for the 4-wire, 56/64-kbps module, use one of the following commands for a serial interface in interface configuration mode.

Command	Purpose

`Router(config-if)# service-module 56k data-coding normal`
or
`Router(config-if)# no service-module 56k data-coding`
	Specifies normal data transmission.

Changing Between Digital Data Service and Switched Dial-Up Modes

To transmit packets in DDS mode or switched dial-up mode using the 4-wire, 56/64-kbps CSU/DSU module, use one of the following commands in interface configuration mode for a serial interface:

Command	Purpose

`Router(config-if)# service-module 56k network-type dds`
or
`Router(config-if)# service-module 56k network-type switched`
	Transmits packets in DDS mode or switched dial-up mode.

Use the **no** form of these commands to transmit from a dedicated leased line in DDS mode. DDS mode is enabled by default for the 4-wire CSU/DSU. Switched mode is enabled by default for the 2-wire CSU/DSU.

In switched mode, you need additional dialer configuration commands to configure dial-out numbers. Before you enable the **service-module 56k network-type switched** command, both CSU/DSUs must use a clock source coming from the line and the clock rate must be configured to **auto** or **56k**. If the clock rate is not set correctly, this command will not be accepted.

The 2-wire and 4-wire, 56/64-kbps CSU/DSU modules use V.25 *bis* dial commands to interface with the router. Therefore, the interface must be configured using the **dialer in-band** command. DTR dial is not supported.

Note Any loopbacks in progress are terminated when switching between modes.

Enabling Acceptance of a Remote Loopback Request

To enable the acceptance of a remote loopback request on a 2- or 4-wire, 56/64-kbps CSU/DSU module, use the following command in interface configuration mode for a serial interface:

Command	Purpose
`Router(config-if)# service-module 56k remote-loopback`	Enables a remote loopback request.

The **no service-module 56k remote-loopback** command prevents the local CSU/DSU from being placed into loopback by remote devices on the line. Unlike the T1 module, the 2- or 4-wire, 56/64-kbps CSU/DSU module can still initiate remote loopbacks with the **no** form of this command configured.

Selecting a Service Provider

To select a service provider to use with a 2- or 4-wire, 56/64 kbps dial-up line, use the following command in interface configuration mode for a serial interface:

Command	Purpose
Router(config-if)# **service-module 56k switched-carrier** {**att** | **other** | **sprint**}	Selects a service provider for a 2- or 4-wire switched, 56/64 kbps dialup line.

The **att** keyword specifies AT&T or another digital network service provider as the line carrier, which is the default for the 4-wire, 56/64-kbps CSU/DSU module. The **sprint** keyword specifies Sprint or another service provider whose network carries mixed voice and data as the line carrier, which is the default for the 2-wire switched 56-kbps CSU/DSU module.

In a Sprint network, echo-canceler tones are sent during call setup to prevent echo cancelers from damaging digital data. The transmission of these cancelers may increase call setup times by 8 seconds on the 4-wire module. Having echo cancellation enabled does not affect data traffic.

This configuration command is ignored if the network type is DDS.

Use the **no** form of this command to enable the default service provider. AT&T is enabled by default on the 4-wire, 56/64 module. Sprint is enabled by default on the 2-wire switched, 56-kbps module.

Configuring Low-Speed Serial Interfaces

This section describes how to configure low-speed serial interfaces. In addition to the background information described in the "Understanding Half-Duplex DTE and DCE State Machines" section on page 288, these sections provide guidelines for configuring low-speed serial interfaces:

- Changing Between Controlled-Carrier and Constant-Carrier Modes, page 292
- Tuning Half-Duplex Timers, page 293
- Changing Between Synchronous and Asynchronous Modes, page 294

For configuration examples, see the "Low-Speed Serial Interface Examples" section on page 316.

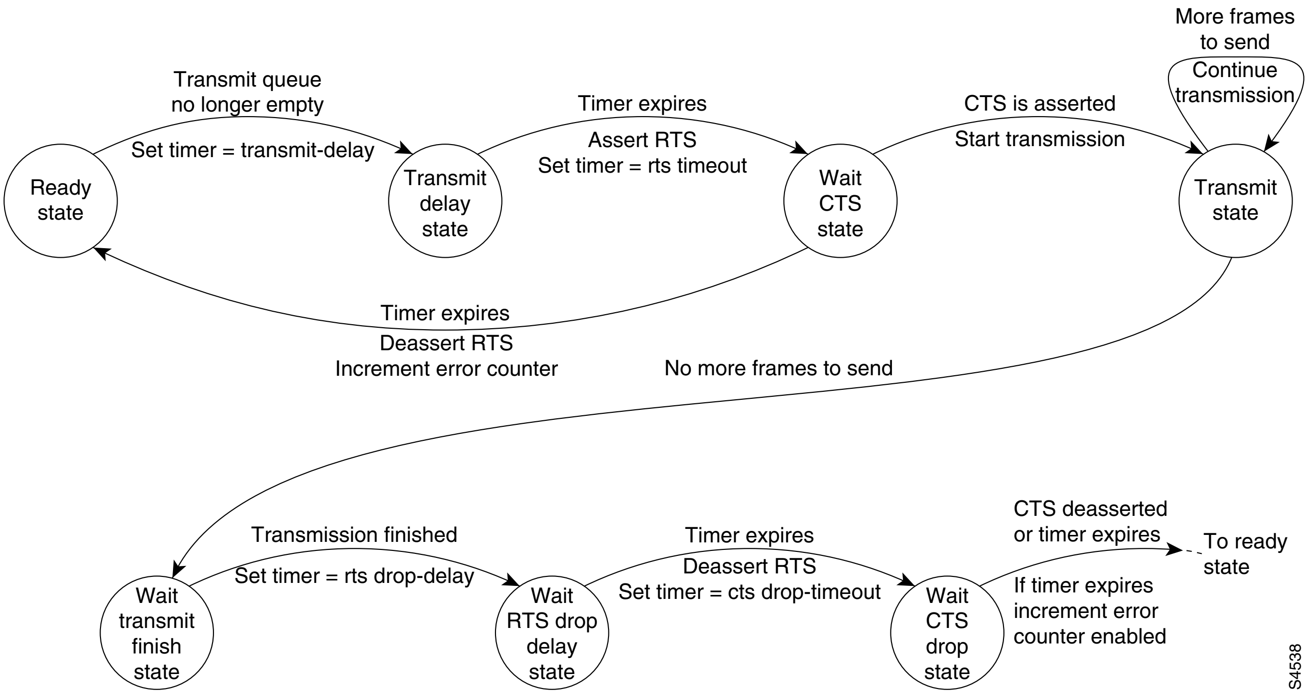
Understanding Half-Duplex DTE and DCE State Machines

The following sections describe the communication between half-duplex DTE transmit and receive state machines and half-duplex DCE transmit and receive state machines.

Half-Duplex DTE State Machines

As shown in Figure 26, the half-duplex DTE transmit state machine for low-speed interfaces remains in the ready state when it is quiescent. When a frame is available for transmission, the state machine enters the transmit delay state and waits for a time period, which is defined by the **half-duplex timer transmit-delay** command. The default is 0 milliseconds. Transmission delays are used for debugging half-duplex links and assisting lower-speed receivers that cannot process back-to-back frames.

Figure 26 Half-Duplex DTE Transmit State Machine



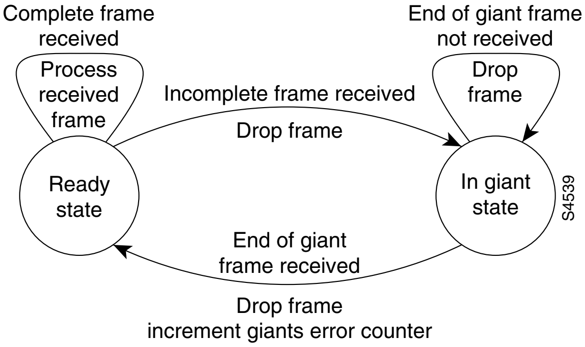
After idling for a defined number of milliseconds (ms), the state machine asserts a request to send (RTS) signal and changes to the wait-clear-to-send (CTS) state for the DCE to assert CTS. A timeout timer with a value set by the **half-duplex timer rts-timeout** command starts. This default is 3 ms. If the timeout timer expires before CTS is asserted, the state machine returns to the ready state and deasserts RTS. If CTS is asserted before the timer expires, the state machine enters the transmit state and sends the frames.

Once there are no more frames to transmit, the state machine transitions to the wait transmit finish state. The machine waits for the transmit FIFO in the serial controller to empty, starts a delay timer with a value defined by the **half-duplex timer rts-drop-delay** interface command, and transitions to the wait RTS drop delay state.

When the timer in the wait RTS drop delay state expires, the state machine deasserts RTS and transitions to the wait CTS drop state. A timeout timer with a value set by the **half-duplex timer cts-drop-timeout** interface command starts, and the state machine waits for the CTS to deassert. The default is 250 ms. Once the CTS signal is deasserted or the timeout timer expires, the state machine transitions back to the ready state. If the timer expires before CTS is deasserted, an error counter is incremented, which can be displayed by issuing the **show controllers** command for the serial interface in question.

As shown in Figure 27, a half-duplex DTE receive state machine for low-speed interfaces idles and receives frames in the ready state. A giant frame is any frame whose size exceeds the maximum transmission unit (MTU). If the beginning of a giant frame is received, the state machine transitions to the in giant state and discards frame fragments until it receives the end of the giant frame. At this point, the state machine transitions back to the ready state and waits for the next frame to arrive.

Figure 27 Half-Duplex DTE Receive State Machine

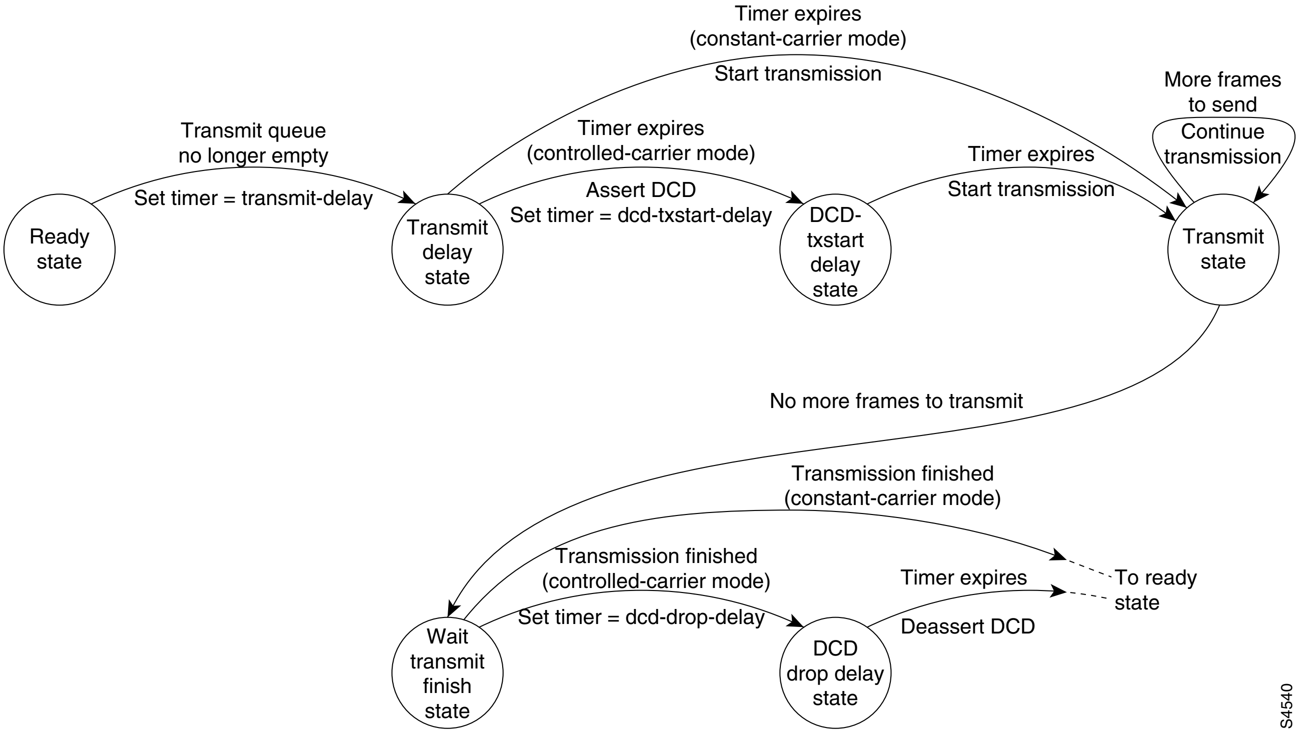

Complete frame received
Process received frame
Incomplete frame received
Drop frame
End of giant frame not received
Drop frame
Ready state
In giant state
S4539
End of giant frame received
Drop frame increment giants error counter

An error counter is incremented upon receipt of the giant frames. To view the error counter, use the **show interfaces** command for the serial interface in question.

Half-Duplex DCE State Machines

As shown in Figure 28, for a low-speed serial interface in DCE mode, the half-duplex DCE transmit state machine idles in the ready state when it is quiescent. When a frame is available for transmission on the serial interface, such as when the output queues are no longer empty, the state machine starts a timer (based on the value of the **half-duplex timer transmit-delay** command, in milliseconds) and transitions to the transmit delay state. Similar to the DTE transmit state machine, the transmit delay state gives you the option of setting a delay between the transmission of frames; for example, this feature lets you compensate for a slow receiver that loses data when multiple frames are received in quick succession. The default **transmit-delay** value is 0 ms; use the **half-duplex timer transmit-delay** interface configuration command to specify a delay value not equal to 0.

Figure 28 Half-Duplex DCE Transmit State Machine



After the transmit delay state, the next state depends on whether the interface is in constant-carrier mode (the default) or controlled-carrier mode.

If the interface is in constant-carrier mode, it passes through the following states:

1. The state machine passes to the transmit state when the **transmit-delay** timer expires. The state machine stays in the transmit state until there are no more frames to transmit.
2. When there are no more frames to transmit, the state machine passes to the wait transmit finish state, where it waits for the transmit FIFO to empty.
3. Once the FIFO empties, the DCE passes back to the ready state and waits for the next frame to appear in the output queue.

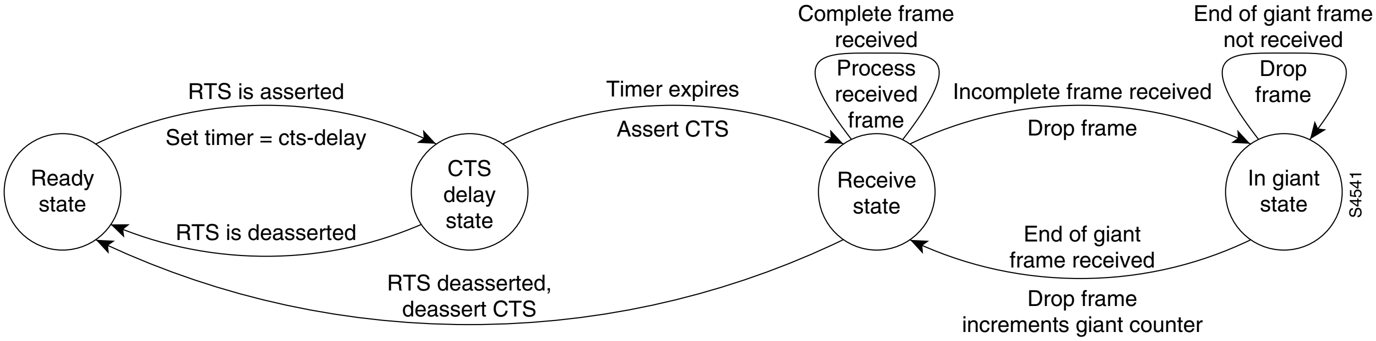
If the interface is in controlled-carrier mode, the interface performs a handshake using the data carrier detect (DCD) signal. In this mode, DCD is deasserted when the interface is idle and has nothing to transmit. The transmit state machine transitions through the states as follows:

1. After the **transmit-delay** timer expires, the DCE asserts DCD and transitions to the DCD-txstart delay state to ensure a time delay between the assertion of DCD and the start of transmission. A timer is started based on the value specified using the **dcd-txstart-delay** command. (This timer has a default value of 100 ms; use the **half-duplex timer dcd-txstart-delay** interface configuration command to specify a delay value.)
2. When this delay timer expires, the state machine transitions to the transmit state and transmits frames until there are no more frames to transmit.
3. After the DCE transmits the last frame, it transitions to the wait transmit finish state, where it waits for transmit FIFO to empty and the last frame to transmit to the wire. Then DCE starts a delay timer by specifying the value using the **dcd-drop-delay** command. (This timer has the default value of 100 ms; use the **half-duplex timer dcd-drop-delay** interface configuration command to specify a delay value.)

4. The DCE transitions to the wait DCD drop delay state. This state causes a time delay between the transmission of the last frame and the deassertion of DCD in the controlled-carrier mode for DCE transmits.
5. When the timer expires, the DCE deasserts DCD and transitions back to the ready state and stays there until there is a frame to transmit on that interface.

As shown in Figure 29, the half-duplex DCE receive state machine idles in the ready state when it is quiescent. It transitions out of this state when the DTE asserts RTS. In response, the DCE starts a timer based on the value specified using the **cts-delay** command. This timer delays the assertion of CTS because some DTE interfaces expect this delay. (The default value of this timer is 0 ms; use the **half-duplex timer cts-delay** interface configuration command to specify a delay value.)

Figure 29 Half-Duplex DCE Receive State Machine



When the timer expires, the DCE state machine asserts CTS and transitions to the receive state. It stays in the receive state until there is a frame to receive. If the beginning of a giant frame is received, it transitions to the in giant state and keeps discarding all the fragments of the giant frame and transitions back to the receive state.

Transitions back to the ready state occur when RTS is deasserted by the DTE. The response of the DCE to the deassertion of RTS is to deassert CTS and go back to the ready state.

Changing Between Controlled-Carrier and Constant-Carrier Modes

The **half-duplex controlled-carrier** command enables you to change between controlled-carrier and constant-carrier modes for low-speed serial DCE interfaces in half-duplex mode. Configure a serial interface for half-duplex mode by using the **half-duplex** command. Full-duplex mode is the default for serial interfaces. This interface configuration is available on Cisco 2520 through Cisco 2523 routers.

Controlled-carrier operation means that the DCE interface will have DCD deasserted in the quiescent state. When the interface has something to transmit, it will assert DCD, wait a user-configured amount of time, then start the transmission. When it has finished transmitting, it will again wait a user-configured amount of time and then deassert DCD.

Placing a Low-Speed Serial Interface in Controlled-Carrier Mode

To place a low-speed serial interface in controlled-carrier mode, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# half-duplex controlled-carrier`	Places a low-speed serial interface in controlled-carrier mode.

Placing a Low-Speed Serial Interface in Constant-Carrier Mode

To return a low-speed serial interface to constant-carrier mode from controlled-carrier mode, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# no half-duplex controlled-carrier`	Places a low-speed serial interface in constant-carrier mode.

Tuning Half-Duplex Timers

To optimize the performance of half-duplex timers, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# half-duplex timer {cts-delay value | cts-drop-timeout value | dcd-drop-delay value | dcd-txstart-delay value | rts-drop-delay value | rts-timeout value | transmit-delay value}`	Tunes half-duplex timers.

The timer tuning commands permit you to adjust the timing of the half-duplex state machines to suit the particular needs of their half-duplex installation.

Note that the **half-duplex timer** command and its options replaces the following two timer tuning commands that are available only on high-speed serial interfaces:

- **sdlc cts-delay**
- **sdlc rts-timeout**

Changing Between Synchronous and Asynchronous Modes

To specify the mode of a low-speed serial interface as either synchronous or asynchronous, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# physical-layer {sync	async}`	Specifies the mode of a low-speed interface as either synchronous or asynchronous.

This command applies only to low-speed serial interfaces available on Cisco 2520 through Cisco 2523 routers.

In synchronous mode, low-speed serial interfaces support all interface configuration commands available for high-speed serial interfaces, except the following two commands:

- **sdlc cts-delay**
- **sdlc rts-timeout**

When placed in asynchronous mode, low-speed serial interfaces support all commands available for standard asynchronous interfaces. The default is synchronous mode.

Note When you use this command, it does not appear in the output of the **show running-config** and **show startup-config** commands, because the command is a physical-layer command.

To return to the default mode (synchronous) of a low-speed serial interface on a Cisco 2520 through Cisco 2523 router, use the following command in interface configuration mode.

Command	Purpose
`Router(config-if)# no physical-layer`	Returns the interface to its default mode, which is synchronous.

Troubleshooting Serial Interfaces

Perform the tasks in this section to troubleshoot issues with serial interfaces:

- Troubleshooting Channelized T1 or E1, page 294
- Troubleshooting the T3 and T1 Channels on the CT3IP, page 297
- Troubleshooting the PA-E3 Port Adapter, page 302

Troubleshooting Channelized T1 or E1

When troubleshooting channelized T1 or E1, you must first determine if the problem is with a particular channel group or with the T1 or E1 line.

If the problem is with a single channel group, you have a potential interface problem.

If the problem is with the T1 or E1 line, or with all channel groups, you have a potential controller problem.

The following section describes how to determine whether the problem affects an interface or a controller:

- Running Controller Loopback Diagnostic Tests, page 295

When you troubleshoot E1 or T1 controllers, first check that the configuration is correct. The framing type and line code should match what the service provider has specified. Then check channel group and PRI-group configurations, especially to verify that the time slots and speeds are what the service provider has specified.

At this point, the **show controllers t1** or **show controllers e1** commands should be used to check for T1 or E1 errors. Use the command several times to determine if error counters are increasing, or if the line status is continually changing. If these errors are occurring, you need to work with the service provider.

Note Cisco routers do not have CSU capability and do not react to any remote loopback codes at the T1 or E1 level.

Running Controller Loopback Diagnostic Tests

Controller loopback tests are a means to isolate problems and are available for both channelized T1 controllers and channelized E1 controllers. The following loopback tests are documented for isolating T1 and E1 controller issues:

- Local Loopback, page 295
- Remote Loopback, page 296
- Channelized E1 Controller Loopback, page 296

Local Loopback

The local loopback loops the controller both toward the router and toward the line. Because the loopback is done internally to the router, the controller should make the transition to the UP state within approximately 10 seconds, and no further T1 errors should be detected.

All channel groups will be looped back; if the encapsulation on that channel group supports loopbacks (for example, HDLC and PPP), you can test that channel group by pinging the interface address. For example, if you have assigned an IP address to the serial interface defined for a channel group, you can ping that IP address.

To place the controller into local loopback, use the following command in controller configuration mode.

Command	Purpose
`Router(config-controller)# `**`loopback local controller`**	Loops the T1 controller toward the router and toward the line.

To test a channel group, use the following command in EXEC mode.

Command	Purpose
`Router# `**`ping`**` `*`protocol protocol-address`*	Pings the interface address.

To check errors, use the following command in EXEC mode.

Command	Purpose
`Router> show controllers t1`	Checks errors.

If any errors occur, or the controller fails to change to the up state, contact the Cisco Technical Assistance Center (TAC).

Because the controller local loopback is bidirectional, the service provider can test the line integrity using a T1 bit error rate tester (BERT) test set.

Remote Loopback

The second T1 controller loopback is a remote loopback. This loopback can be used only if the *entire* T1 goes to a remote CSU. This is not the case with 99.9 percent of channelized T1. When the **loopback remote controller** command is executed, an in-band CSU loop-up code will be sent over the entire T1, which will attempt to loop up the remote CSU. To place the controller in remote loopback, use the following command in controller configuration mode.

Command	Purpose
`Router(config-controller)# loopback remote controller`	Places the T1 controller in remote loopback.

Note If controller loopbacks are used, they will disrupt service for all channel groups on that interface.

Channelized E1 Controller Loopback

For the E1 controller, only the local loopback is available. Local loopback operates the same as the local loopback on the T1 controller, forming a bidirectional loopback, both toward the router and toward the line. To place the E1 controller in local loopback, use the following command in controller configuration mode.

Command	Purpose
`Router(config-controller)# loopback controller`	Places the E1 controller in local loopback toward the router and toward the line.

All channel groups will be looped back; if the encapsulation on that channel group supports loopbacks (for example, HDLC and PPP), you can test that channel group by pinging the interface address. For example, if you have assigned an IP address to the serial interface defined for a channel group, you can ping that IP address.

To place the controller into local loopback, use the following command in controller configuration mode.

Command	Purpose
`Router(config-controller)# loopback local controller`	Loops the T1 controller toward the router and toward the line.

To test a channel group, use the following command in EXEC mode.

Command	Purpose
`Router> ping protocol protocol-address`	Pings the interface address.

To check errors, if any, use the following command in EXEC mode.

Command	Purpose
`Router> show controllers t1`	Checks errors.

If any errors occur, they are most likely a hardware problem; contact the Cisco TAC. In addition, you can ask the service provider to test the line by using a T1 BERT test set.

Troubleshooting the T3 and T1 Channels on the CT3IP

To troubleshoot the CT3IP using Cisco IOS software, use the following methods:

- Test the T1 by using the **t1 test** controller configuration command and the test port.
- Loop the T1 by using **loopback** interface configuration commands.
- Loop the T3 by using **loopback** controller configuration commands.

Enabling Test Port

You can use the T1 test port available on the CT3IP to break out any of the 28 T1 channels for testing (for example, 24-hour bit error rate tester (BERT) testing is commonly done by telephone companies before a line is brought into service).

The T1 test port is also available as an external port. For more information on configuring an external port, see the "Configuring External T1 Channels" section on page 258.

Note If a T1 channel that was previously configured as a serial interface is broken out to the T1 port test, then that interface and its associated configuration remain intact while the channel is broken out to the T1 port test. The serial interface is not usable during the time the T1 channel is broken out to the T1 test port; however, the configuration remains to facilitate the return of the T1 channel to a serial interface using the **no t1 test** command.

To enable a T1 channel as a test port, use the following commands beginning in privileged EXEC mode.

	Command	Purpose
Step 1	`Router# show controller t3 slot/port-adapter/port`	Displays the Ext1... field so that you can verify whether the external device connected to the external T1 port is configured and cabled correctly. If the line status is OK, a valid signal is being received and the signal is not an all-ones signal.

	Command	Purpose
Step 2	Router(config)# **controller t3** *slot*/*port-adapter*/*port*	Selects the CT3IP and enters controller configuration mode.
Step 3	Router(config-controller)# **t1 test** *channel* [**cablelength** *feet*] [**linecode** {**ami** | **b8zs**}]	Enables the T1 channel (values are 1 to 28) as a test port and optionally specifies the cable length and line code. The default **cablelength** is 133 feet, and the default **linecode** is **b8zs**.

To disable a T1 channel as a test port, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# **controller t3** *slot*/*port-adapter*/*port*	Selects the CT3IP and enters controller configuration mode.
Step 2	Router(config-controller)# **no t1 test** *channel*	Disables the T1 channel (values are 1 to 28) as a test port.

Note Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

Loopback T1 Channels

You can perform the following types of loopbacks on a T1 channel:

- Local—Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) out toward the network (see Figure 30).
- Network line—Loops the data back toward the network before the T1 framer and automatically sets a local loopback (see Figure 31).
- Network payload—Loops just the payload data back toward the network at the T1 framer and automatically sets a local loopback (see Figure 32).
- Remote line inband—Sends a repeating 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback (see Figure 33).

To enable loopbacks on a T1 channel, use the first command in global configuration mode, followed by any one of the following commands in interface configuration mode.

	Command	Purpose
Step 1	`Router(config)# interface serial slot/port-adapter/port:t1-channel`	Selects the T1 channel (values are 1 to 28) on the CT3IP and enters interface configuration mode.
Step 2	`Router(config-if)# loopback local`	Enables the local loopback on the T1 channel.
	`Router(config-if)# loopback network line`	Enables the network line loopback on the T1 channel.
	`Router(config-if)# loopback network payload`	Enables the network payload loopback on the T1 channel.
	`Router(config-if)# loopback remote line inband`	Enables the remote line inband loopback on the T1 channel.

Note The port adapter and port numbers for the CT3IP are 0.

Figure 30 shows an example of a local loopback in which the loopback occurs in the T1 framer.

Figure 30 CT3IP Local Loopback

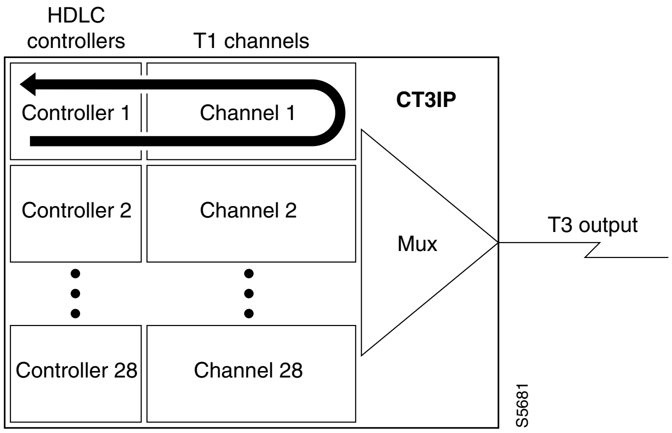


Figure 31 shows an example of a network line loopback in which just the data is looped back toward the network (before the T1 framer).

Figure 31 CT3IP Network Line Loopback

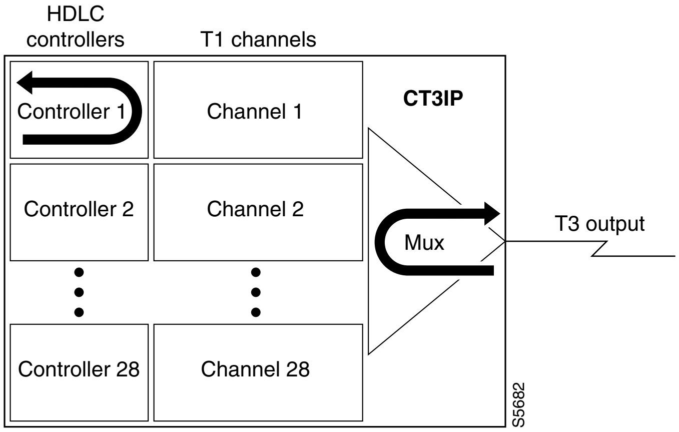


Figure 32 shows an example of a network payload loopback in which just the payload data is looped back toward the network at the T1 framer.

Figure 32 CT3IP Network Payload Loopback

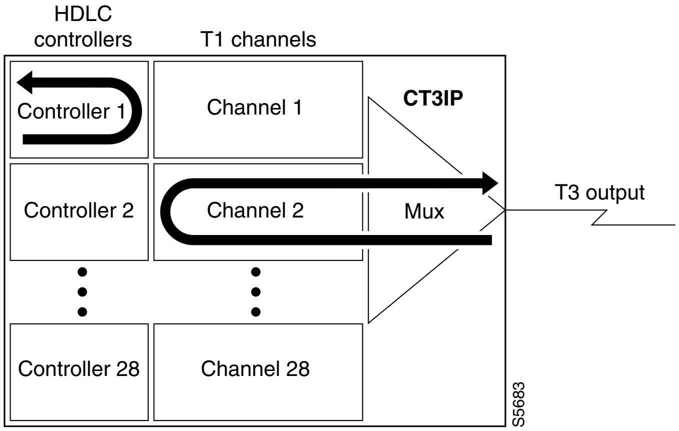
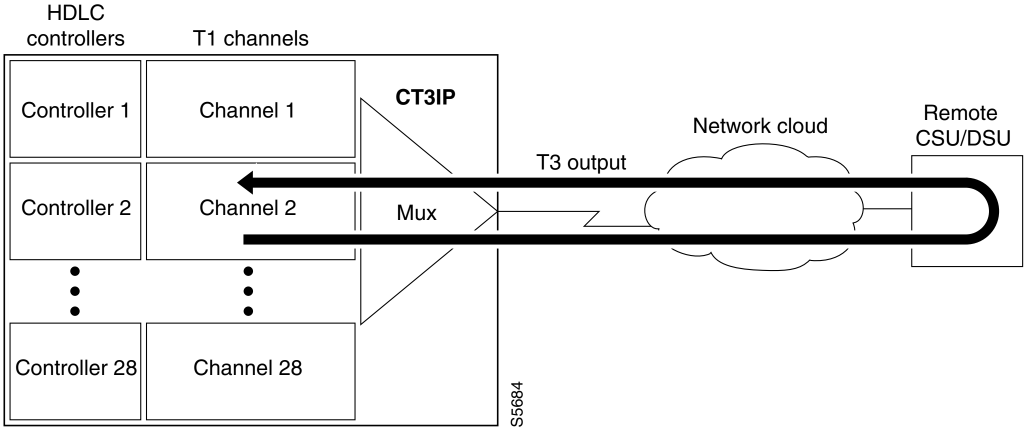


Figure 33 shows an example of a remote inband loopback in which the network line enters a line loopback.

Figure 33 CT3IP Remote Loopback



Loopback T3 Lines

You can put the entire T3 line into loopback mode (that is, all T1 channels are looped) by using the following types of loopbacks:

- Local—Loops the router output data back toward the router at the T1 framer and sends an AIS signal out toward the network.
- Network—Loops the data back toward the network (before the T1 framer).
- Remote—Sends a FEAC (far-end alarm control) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. The type of framing used is determined by the equipment to which you are connected. (For more information, refer to the **framing** controller configuration command in the *Cisco IOS Interface and Hardware Component Command Reference*.)

To enable loopbacks on the T3 (and all T1 channels), use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)# controller t3 slot/port-adapter/port`	Selects the CT3IP and enters controller configuration mode. The port adapter and port numbers for the CT3IP are 0.
Step 2	`Router(config-controller)# loopback local`	(Optional) Enables the local loopback.
	`Router(config-controller)# loopback network`	(Optional) Enables the network loopback.
	`Router(config-controller)# loopback remote`	(Optional) Enables the remote loopback.

Troubleshooting the PA-E3 Port Adapter

To set the following loopbacks to troubleshoot the PA-E3 port adapter using Cisco IOS software, use the first command in global configuration mode, followed by any of the other commands, depending on your needs:

Command	Purpose
`Router(config)# loopback dte`	Loops back after the line interface unit (LIU) toward the terminal.
`Router(config)# loopback local`	Loops back after going through the framer toward the terminal.
`Router(config)# loopback network line`	Loops back toward the network before going through the framer.
`Router(config)# loopback network payload`	Loops back toward the network after going through the framer.

These loopback commands loop all packets from the E3 interface back to the interface and also direct the packets to the network.

Serial Interface Configuration Examples

This section provides the following examples:

- Interface Enablement Configuration Examples, page 302
- HSSI Configuration Examples, page 303
- Channelized T3 Interface Processor Configuration Examples, page 303
- PA-E3 Serial Port Adapter Configuration Example, page 307
- PA-T3 and PA-2T3 Configuration Example, page 307
- Packet OC-3 Interface Configuration Examples, page 307
- DPT OC-12c Interface Configuration Examples, page 308
- APS Configuration Examples, page 309
- CSU/DSU Service Module Examples, page 312
- Low-Speed Serial Interface Examples, page 316

Interface Enablement Configuration Examples

The following example illustrates how to begin interface configuration on a serial interface. It assigns PPP encapsulation to serial interface 0.

```
interface serial 0
 encapsulation ppp
```

The same example on a Cisco 7500 The same example on a Cisco 7500 series router, assigning PPP encapsulation to port 0 in slot 1, requires the following commands:

```
interface serial 1/0
 encapsulation ppp
```

This example shows how to configure the access server so that it will use the default address pool on all interfaces except interface 7, on which it will use an address pool called lass:

```
ip address-pool local
ip local-pool lass 172.30.0.1
 async interface
 interface 7
 peer default ip address lass
```

HSSI Configuration Examples

The following example shows a simple configuration for a HSSI port adapter on a Cisco 7500 series router:

```
interface hssi 2/0/0
 ip address 10.1.1.10 255.255.255.0
 description To San Jose, circuit ID 1234
 no ip mroute-cache
```

The following example shows how to configure a 1-port HSSI network module on a Cisco 3600 series router. Both sides of the network connection need to be configured:

```
interface hssi 0/0
! Specifies a HSSI interface; changes from global configuration mode to interface 
configuration mode.
 ip address 10.1.1.1 255.255.255.0
 ! Assigns IP address 10.1.1.1 to the interface.
 hssi internal-clock
 ! Converts the HSSI interface into a clock master.
 no fair-queue
 ! Disables weighted fair queueing (WFQ).
 no shutdown
 ! Enables the port.

interface hssi 1/0
 ip address 10.1.1.2 255.255.255.0
 hssi internal-clock
 no fair-queue
 no shutdown
```

Channelized T3 Interface Processor Configuration Examples

The examples in this section show how to configure the Channelized T3 Interface Processor (CT3IP). The first example shows how to configure two of the T1 channels of the channelized T3 controller. The second example shows how to configure one of the T1 channels of the channelized T3 controller as an external port for further channelization on the Multichannel Interface Processor (MIP).

For more information, see the "Configuring T3 Controller Support for the Cisco AS5800" section on page 255, the "Configuring the T3 Controller" section on page 255, and the "Configuring External T1 Channels" section on page 258. The following examples are included in this section:

- Typical CT3IP Controller Configuration Examples, page 304
- CT3IP Configuration with Default Values Accepted Example, page 305

- CT3IP External Ports Configuration Example, page 305
- CT3IP Maintenance Data Link Example, page 306
- CT3IP Performance Monitoring Example, page 306
- BERT Profile Configuration Example, page 306
- E2 Clock Rate Configuration Example, page 306
- CT3IP BERT Test Pattern Example, page 306
- CT3IP Remote FDL Loopback Example, page 306

Typical CT3IP Controller Configuration Examples

A typical T3 controller configuration in a running-configuration file follows:

```
T3 controller configuration:
----------------------------
controller T3 1/0/0
 framing m23
 clock source line
 cablelength 224
 t1 1 controller
 t1 2 controller
 t1 3 controller
 t1 4 controller
 t1 5 controller
 t1 6 controller
 t1 7 controller
 t1 8 controller
 t1 9 controller
 t1 10 controller
 t1 11 controller
 t1 12 controller
 t1 13 controller
 t1 14 controller
 t1 15 controller
 t1 16 controller
 t1 17 controller
 t1 18 controller
 t1 19 controller
 t1 20 controller
 t1 21 controller
 t1 22 controller
 t1 23 controller
 t1 24 controller
 t1 25 controller
 t1 26 controller
 t1 27 controller
 t1 28 controller
```

A typical T1 controller configuration follows:

```
T1 controller configuration:
----------------------------
controller T1 1/0/0:1
 framing esf
 pri-group timeslots 1-24
 controller T1 1/0/0:2
 channel-group 0 timeslots 1-24
           .
           .
           .
controller T1 1/1/0:28
cas-group 0 timeslots 1-24
```

CT3IP Configuration with Default Values Accepted Example

In the following example, time slots and IP addresses are assigned to channels for the CT3IP in slot 9. (The default framing, cable length, and clock source are accepted for the T3, and the default speed, framing, clock source, and line code are accepted for each T1 channel.)

```
controller t3 9/0/0
 t1 16 timeslot 1-24
 ! Assigns time slots 1 through 24 (the entire T1 bandwidth) to T1 channel 16.
 t1 10 timeslot 1-5,20-23
 ! Assigns time slots 1 through 5 and 20 through 23 (fractional T1 bandwidth)
 ! to T1 channel 10.
interface serial 9/0/0:16
 ip address 10.20.20.1 255.255.255.0
 ! Assigns IP address 10.20.20.1 to T1 channel 16.
interface serial 9/0/0:10
 ip address 10.20.20.3 255.255.255.0
 ! Assigns IP address 10.20.20.3 to T1 channel 10.
 ! Other interface configuration commands can be assigned to the T1 channel
 ! at this time.
```

CT3IP External Ports Configuration Example

In the following example, T1 channel 1 on the CT3IP in slot 9 is broken out as an external port:

```
controller t3 9/0/0
 t1 external 1 cablelength 300
 ! Breaks out T1 channel 1 as an external port so that it can be further channelized on
 ! the MIP in slot 3.
 ! Cable length is set to 300 feet.
 ! The default line coding format (B8ZS) is used for the T1 channel.
controller t1 3/0
 linecode b8zs
 ! The line coding on the MIP is changed to B8ZS to match the line coding on the
 ! T1 channel.
 channel-group 1 timeslots 1
interface serial 3/0:1
 ip address 10.20.20.5 255.255.255.0
```

CT3IP Maintenance Data Link Example

The following examples show several of the Maintenance Data Link (MDL) messages for the CT3IP in slot 9:

```
controller t3 9/0/0
 mdl string eic Router C
 mdl string lic Network A
 mdl string fic Bldg 102
 mdl string unit 123ABC
```

CT3IP Performance Monitoring Example

In the following example, the performance reports are generated for T1 channel 6 on the CT3IP in slot 9:

```
controller t3 9/0/0
 t1 6 fdl ansi
```

BERT Profile Configuration Example

The following example shows a configured BERT profile number 1 that has a 0s test pattern, with a 10^{-2} threshold, no error injection, and a duration of 125 minutes:

```
bert profile 1 pattern 0s threshold 10^-2 error-injection none duration 125
```

E2 Clock Rate Configuration Example

The following example shows output when the e2 clock rate is configured using the **e2-clockrate** EXEC command:

```
Router# e2-clockrate

 Interface Serial 0 is configured to support clockrates up to E2 (8Mbps)
 Interfaces serial 1-3 will not be operational
```

CT3IP BERT Test Pattern Example

The following example shows how to enable a BERT test pattern that consists of a repeating pattern of ones (...111...) and that runs for 30 minutes for T1 channel 8 on CT3IP in slot 9:

```
controller t3 9/0/0
 t1 8 bert pattern 1s interval 30
```

CT3IP Remote FDL Loopback Example

The following example shows how to enable a remote payload FDL ANSI bit loopback for T1 channel 6 on CT3IP in slot 3:

```
interface serial 3/0/0:6
 loopback remote payload fdl ansi
```

PA-E3 Serial Port Adapter Configuration Example

The following example shows a typical configuration for serial interface 1/0/0 on a PA-E3 serial port adapter in a Cisco 7500 series router:

```
interface serial 1/0/0
 ip address 10.1.1.10 255.255.255.0
 clock source internal
 crc 32
 dsu bandwidth 16000
 ! Reduces the bandwidth by padding the E3 frame.
 dsu mode 0
 ! Enables and improves interoperability with other DSUs.
 national bit 1
 ! Sets bit 12 in the E3 frame to 1.
 no scramble
 framing g751
 no shutdown
```

PA-T3 and PA-2T3 Configuration Example

The following example shows a typical configuration for serial interface 1/0/0 on a PA-T3 serial port adapter in a Cisco 7500 series router:

```
interface serial 1/0/0
 ip address 1.1.1.10 255.255.255.0
 clock source internal
 crc 32
 dsu bandwidth 16000
 ! Reduces the bandwidth by padding the E3 frame.
 dsu mode 0
 ! Enables and improves interoperability with other DSUs.
 no scramble
 framing c-bit
 no shutdown
```

Packet OC-3 Interface Configuration Examples

The examples in this section include a simple configuration and a more complex configuration for two routers back to back.

Packet-Over-SONET OC-3 Configuration

This example shows a POS interface in slot 0, port adapter slot 0, port 0 on a Cisco 7500 series router:

```
interface POS0/0/0
 ip address 10.1.1.4 255.255.255.0
 ip route-cache distributed
 no keepalive
 clock source internal
 pos report rdool
 pos report lais
 pos report lrdi
 pos report pais
 pos report prdi
 pos report sd-ber
 no cdp enable
```

Packet OC-3 Configuration with Default Values Accepted Example

In the following example, the default framing, MTU, and clock source are accepted, and the interface is configured for the IP protocol:

```
interface pos 3/0
 ip address 172.18.2.3 255.0.0.0
```

Two Routers Connected Back-to-Back Example

To connect two routers, attach the cable between the Packet OC-3 port on each. By default, the POS uses loop timing mode. For back-to-back operation, only one of the POSs may be configured to supply its internal clock to the line.

In the following example, two routers are connected back-to-back through their Packet OC-3 interfaces:

First Router

```
interface pos 3/0
 ip address 172.18.2.3 255.0.0.0
 no keepalive
 pos internal-clock
```

Second Router

```
interface pos 3/0
 ip address 172.18.2.4 255.0.0.0
 no keepalive
```

The following example shuts down the entire T1 line physically connected to a Cisco 7500 series routers:

```
controller t1 4/0
 shutdown
```

DPT OC-12c Interface Configuration Examples

This section provides the following configuration examples:

- DPT Port Adapter Configuration Example, page 308
- DPT Interface Processor Configuration Example, page 308
- IPS Options Configuration Example, page 309
- DPT Topology Configuration Example, page 309

DPT Port Adapter Configuration Example

In the following example, the OC-12c DPT SRP interface is specified, and the IP address and subnet mask are assigned to the interface.

```
interface srp 0/1
 ip address 192.168.2.3 255.255.255.0
```

DPT Interface Processor Configuration Example

In the following example, the OC-12c DPTIP SRP interface is specified, and the IP address and subnet mask is assigned to the interface.

```
interface srp 0/1/0
 ip address 192.168.2.3 255.255.255.0
```

IPS Options Configuration Example

In the following example, the SRP IPS options are configured on a DPT interface:

```
interface srp 2/0
 srp ips request manual-switch a
 srp ips wtr-timer 60
 srp ips timer 90
```

DPT Topology Configuration Example

In the following example, the identity of the nodes on the DPT ring according to their MAC addresses is shown. The following example shows a three-node DPT ring.

```
Router# show srp topology

Topology Map for Interface SRP2/0
  Topology pkt. sent every 5 sec. (next pkt. after 4 sec.)
  Last received topology pkt. 00:00:00
  Nodes on the ring:4
  Hops (outer ring)      MAC       IP Address      Wrapped Name
      0             0000.0000.0004 10.2.2.4           No    stingray
      1             0000.0000.0001 10.2.2.1           No    npe300
      2             0000.0000.0005 10.2.2.5           No    gsr
      3             0000.0000.0002 10.2.2.2           No    tuna
```

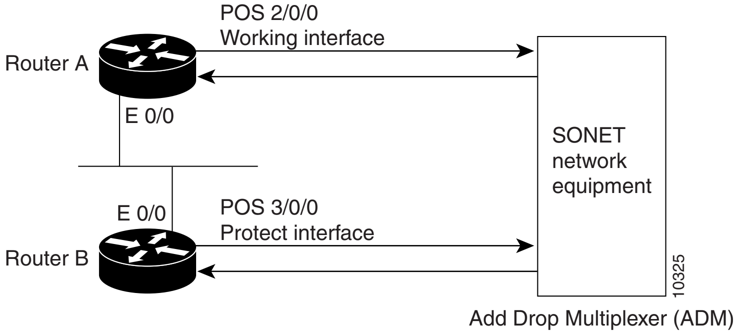
APS Configuration Examples

The following examples show how to configure basic APS on a router and how to configure more than one protect/working interface on a router by using the **aps group** command.

Basic APS Configuration Example

The following example shows the configuration of APS on Router A and Router B (see Figure 34). In this example, Router A is configured with the working interface, and Router B is configured with the protect interface. If the working interface on Router A becomes unavailable, the connection will automatically switch over to the protect interface on Router B.

Figure 34 Basic APS Configuration



On Router A, which contains the working interface, use the following configuration:

```
interface ethernet 0/0
 ip address 10.7.7.7 255.255.255.0
interface pos 2/0/0
 aps working 1
```

On Router B, which contains the protect interface, use the following configuration:

```
interface ethernet 0/0
 ip address 10.7.7.6 255.255.255.0
interface pos 3/0/0
 aps protect 1 10.7.7.7
```

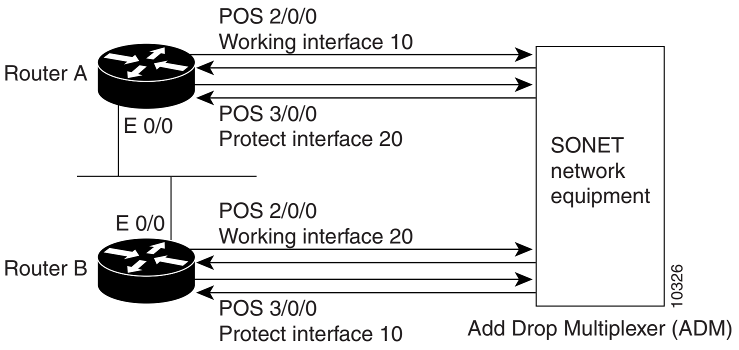
To verify the configuration or to determine if a switchover has occurred, use the **show aps** command.

Multiple APS Interfaces Configuration Example

To configure more than one protect/working interface on a router, you must use the **aps group** command. The following example shows the configuration of grouping more than one working/protect interface on a router (see Figure 35). In this example, Router A is configured with a working interface and a protect interface, and Router B is configured with a working interface and a protect interface. Consider the following scenarios:

- If the working interface 2/0/0 on Router A becomes unavailable, the connection will switch over to the protect interface 3/0/0 on Router B because they are both in APS group 10.
- If the working interface 2/0/0 on Router B becomes unavailable, the connection will switch over to the protect interface 3/0/0 on Router A because they are both in APS group 20.

Figure 35 Multiple Working and Protect Interfaces Configuration



Note To avoid the protect interface becoming the active circuit and disabling the working circuit when it is discovered, configure the working interface before configuring the protect interface.

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

```
interface ethernet 0/0
 ip address 10.7.7.6 255.255.255.0
interface pos 2/0/0
aps group 10
 aps working 1
interface pos 3/0/0
 aps group 20
 aps protect 1 10.7.7.7
```

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

```
interface ethernet 0/0
 ip address 10.7.7.7 255.255.255.0
interface pos 2/0/0
aps group 20
 aps working 1
interface pos 3/0/0
 aps group 10
 aps protect 1 10.7.7.6
```

To verify the configuration or to determine if a switchover has occurred, use the **show aps** command.

CSU/DSU Service Module Examples

This section includes three main categories of service module examples:

- FT1/T1 Examples, page 312
- 2- and 4-Wire, 56/64-kbps Service Module Examples, page 314
- E1-G.703/G.704 Serial Port Adapter Example, page 316

FT1/T1 Examples

FT1/T1 examples are provided for these configurations:

- T1 Frame Type Example, page 312
- CSU Line Build-Out Example, page 312
- T1 Line-Code Type Example, page 312
- Loop Codes Example, page 312
- Time Slots Example, page 313
- Performance Report Example, page 313
- Loopback Line Enablement Examples, page 313
- Loopback DTE Examples, page 314
- Clock Source Example, page 314
- TI CSU WIC Configuration Example, page 314

T1 Frame Type Example

The following example enables Superframe as the FT1/T1 frame type:

```
service-module t1 framing sf
```

CSU Line Build-Out Example

The following example shows a line build-out setting of –7.5 dB:

```
service-module t1 lbo -7.5db
```

T1 Line-Code Type Example

The following example specifies AMI as the line-code type:

```
service-module t1 linecode ami
```

Loop Codes Example

The following example displays the configuration of two routers connected back-to-back through an FT1/T1 line and the corresponding feedback messages:

```
no service-module t1 remote-loopback full
service-module t1 remote-loopback payload alternate

loopback remote full
%SERVICE_MODULE-5-LOOPUPFAILED: Unit 0 - Loopup of remote unit failed
```

```
service-module t1 remote-loopback payload v54
loopback remote payload
%SERVICE_MODULE-5-LOOPUPFAILED: Unit 0 - Loopup of remote unit failed

service-module t1 remote-loopback payload alternate
loopback remote payload
%SERVICE_MODULE-5-LOOPUPREMOTE: Unit 0 - Remote unit placed in loopback
```

Time Slots Example

The following example configures a series of time-slot ranges and a speed of 64 kbps:

```
service-module t1 timeslots 1-10,15-20,22 speed 64
```

Performance Report Example

The following is sample output from the **show service-module** serial interface command:

```
Router# show service-module serial 0

Module type is T1/fractional
    Hardware revision is B, Software revision is 1.1i,
    Image checksum is 0x21791D6, Protocol revision is 1.1
Receiver has AIS alarm,
Unit is currently in test mode:
    line loopback is in progress
Framing is ESF, Line Code is B8ZS, Current clock source is line,
Fraction has 24 timeslots (64 Kbits/sec each), Net bandwidth is 1536 Kbits/sec.
Last user loopback performed:
    remote loopback
    Failed to loopup remote
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:05:50
    loss of signal        :    1, last occurred 0:01:50
    loss of frame         :    0,
    AIS alarm             :    1, current duration 0:00:49
    Remote alarm          :    0,
    Module access errors  :    0,
Total Data (last 0 15 minute intervals):
    1466 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (351 seconds elapsed):
    1466 Line Code Violations, 0 Path Code Violations
    25 Slip Secs, 49 Fr Loss Secs, 40 Line Err Secs, 1 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 49 Unavail Secs
```

Loopback Line Enablement Examples

The following example shows how to configure a payload loopback:

```
loopback line payload
 Loopback in progress
no loopback line
```

The following example shows the output when you loop a packet in switched mode without an active connection:

```
service-module 56k network-type switched
loopback line payload
 Need active connection for this type of loopback
 % Service module configuration command failed: WRONG FORMAT.
```

Loopback DTE Examples

The following example loops a packet from a module to the serial interface:

```
loopback dte
 Loopback in progress
ping 10.0.0.1
 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echoes to 10.0.0.1, timeout is 2 seconds:
!!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/28 ms
```

Clock Source Example

The following example shows a router using internal clocking while transmitting frames at 38.4 kbps:

```
service-module 56k clock source internal
service-module 56k clock rate 38.4
```

TI CSU WIC Configuration Example

The following example shows how to set the **fdl** parameter to **att** while in interface configuration mode:

```
interface Serial0/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 no keepalive
 shutdown
 no fair-queue
 service-module t1 clock source internal
 service-module t1 fdl att
 no cdp enable
```

2- and 4-Wire, 56/64-kbps Service Module Examples

This section provides the following examples for 2- and 4-wire, 56/64-kbps service modules:

- Network Line Speed Examples, page 314
- Scrambled Data Coding Example, page 315
- Switched Dial-Up Mode Example, page 315
- Performance Report Example, page 315
- Remote Loopback Request Example, page 316
- Service Provider Example, page 316

Network Line Speed Examples

The following example displays the configuration of two routers connected in back-to-back DDS mode. However, the configuration fails because the **auto** rate is used, which is not valid in back-to-back mode.

```
Router1# service-module 56k clock source internal
Router1# service-module 56k clock rate 38.4

Router2# service-module 56k clock rate auto
% WARNING - auto rate will not work in back-to-back DDS.
```

```
a1# ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router2# service-module 56k clock rate 38.4

Router1# ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
```

When transferring from DDS mode to switched mode, you must set the correct clock rate, as shown in the following example:

```
service-module 56k network-type dds
service-module 56k clock rate 38.4
service-module 56k network-type switched
% Have to use 56k or auto clock rate for switched mode
% Service module configuration command failed: WRONG FORMAT.

service-module 56k clock rate auto
% WARNING - auto rate will not work in back-to-back DDS.
service-module 56k network-type switched
```

Scrambled Data Coding Example

The following example scrambles bit codes in 64-kbps DDS mode:

```
service-module 56k clock rate 56
service-module 56k data-coding scrambled
Can configure scrambler only in 64k speed DDS mode
% Service module configuration command failed: WRONG FORMAT.

service-module 56k clock rate 64
service-module 56k data-coding scrambled
```

Switched Dial-Up Mode Example

The following example displays transmission in switched dial-up mode:

```
service-module 56k clock rate 19.2
service-module 56k network-type switched
% Have to use 56k or auto clock rate for switched mode
% Service module configuration command failed: WRONG FORMAT.

service-module 56k clock rate auto
service-module 56k network-type switched
dialer in-band
dialer string 2576666
dialer-group 1
```

Performance Report Example

The following is sample output from the **show service-module serial** command:

```
Router# show service-module serial 1

Module type is 4-wire Switched 56
    Hardware revision is B, Software revision is X.07,
    Image checksum is 0x45354643, Protocol revision is 1.0
```

```
Connection state: active,
Receiver has loss of signal, loss of sealing current,
Unit is currently in test mode:
    line loopback is in progress
Current line rate is 56 Kbits/sec
Last user loopback performed:
    dte loopback
    duration 00:00:58
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:13:54
    oos/oof              :    3, last occurred 0:00:24
    loss of signal       :    3, current duration 0:00:24
    loss of sealing curren:    2, current duration 0:04:39
    loss of frame        :    0,
    rate adaption attempts:    0,
```

Remote Loopback Request Example

The following example enables you to transmit and receive remote loopbacks:

```
service-module 56k remote-loopback
```

Service Provider Example

The following example selects AT&T as the service provider:

```
service-module 56k network-type switched
service-module 56k switched-carrier att
```

E1-G.703/G.704 Serial Port Adapter Example

The following example shows a configuration for serial interface 9/1/3 on a E1-G.703/G.704 serial port adapter in a Cisco 7500 series router. In this example, the interface is configured for framed (G.704) operation, and time slot 16 is used for data.

```
interface serial 9/1/3
 ip address 10.1.1.10 255.255.255.0
 no keepalive
 no fair-queue
 timeslot 1-31
 crc4
 ts16
```

Low-Speed Serial Interface Examples

The section includes the following configuration examples for low-speed serial interfaces:

- Synchronous or Asynchronous Mode Examples, page 317
- Controlled-Carrier and Constant-Carrier Mode Examples, page 317
- Half-Duplex Timers Example, page 317
- Cisco 4000 Series Router with 2T16S Serial Network Processor Examples, page 318

Synchronous or Asynchronous Mode Examples

The following example shows how to change a low-speed serial interface from synchronous to asynchronous mode:

```
interface serial 2
 physical-layer async
```

The following examples show how to change a low-speed serial interface from asynchronous mode back to its default synchronous mode:

```
interface serial 2
 physical-layer sync
```

or

```
interface serial 2
 no physical-layer
```

The following example shows some typical asynchronous interface configuration commands:

```
interface serial 2
 physical-layer async
 ip address 10.0.0.2 255.0.0.0
 async default ip address 10.0.0.1
 async mode dedicated
 async default routing
```

The following example shows some typical synchronous serial interface configuration commands available when the interface is in synchronous mode:

```
interface serial 2
 physical-layer sync
 ip address 10.0.0.2 255.0.0.0
 no keepalive
 ignore-dcd
 nrzi-encoding
 no shutdown
```

Controlled-Carrier and Constant-Carrier Mode Examples

The following example shows how to change to controlled-carrier mode from the default of constant-carrier operation:

```
interface serial 2
 half-duplex controlled-carrier
```

The following example shows how to change to constant-carrier mode from controlled-carrier mode:

```
interface serial 2
 no half-duplex controlled-carrier
```

Half-Duplex Timers Example

The following example shows how to set the cts-delay timer to 1234 ms and the transmit-delay timer to 50 ms:

```
interface serial 2
 half-duplex timer cts-delay 1234
 half-duplex timer transmit-delay 50
```

Cisco 4000 Series Router with 2T16S Serial Network Processor Examples

The 2T16S network processor module provides high-density serial interfaces for the Cisco 4000 series routers. This module has two high-speed interfaces that support full-duplex T1 and E1 rates (up to 2 MB per second) and 16 low-speed interfaces. The 16 lower-speed ports can be individually configured as either as synchronous ports at speeds up to 128 kbps or as asynchronous ports at speeds up to 115 kbps.

For the low-speed interfaces, both synchronous and asynchronous serial protocols are supported. For the high-speed interfaces, only the synchronous protocols are supported. Synchronous protocols include IBM’s Bisync, SDLC, and HDLC. Asynchronous protocols include PPP, SLIP, and ARAP for dial-up connections using external modems.

The following example shows a Cisco 4500 router equipped with two 2T16S serial network processor modules and two conventional Ethernet ports. The router is configured for WAN aggregation using X.25, Frame Relay, PPP, and HDLC encapsulation. Serial interfaces 0, 1, 18, and 19 are the synchronous high-speed interfaces. Serial interfaces 2 through 17 and 20 through 35 are the synchronous/asynchronous low-speed interfaces.

```
version 11.2
!
hostname c4X00
!
username brad password 7 13171F1D0A080139
username jim password 7 104D000A0618
!
```

Ethernet interfaces and their subinterfaces are configured for LAN access.

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
 media-type 10BaseT
 !
interface Ethernet1
 ip address 10.1.2.1 255.255.255.0
 media-type 10BaseT
 !
```

Serial interfaces 0 and 1 are the high-speed serial interfaces on the first 2T16S module. In this example, subinterfaces are also configured for remote offices connected in to serial interface 0:

```
interface Serial0
 description Frame Relay configuration sample
 no ip address
 encapsulation frame-relay
!
interface Serial0.1 point-to-point
 description PVC to first office
 ip address 10.1.3.1 255.255.255.0
 frame-relay interface-dlci 16
!
interface Serial0.2 point-to-point
 description PVC to second office
 ip address 10.1.4.1 255.255.255.0
 frame-relay interface-dlci 17
!
interface Serial1
 description X25 configuration sample
 ip address 10.1.5.1 255.255.255.0
 no ip mroute-cache
 encapsulation x25
 x25 address 6120184321
 x25 htc 25
 x25 map ip 10.1.5.2 6121230073
```

Serial interfaces 2 to 17 are the low-speed interfaces on the 2T16S network processor module. In this example, remote routers are connected to various configurations.

```
interface Serial2
 description DDR connection router dial out to remote sites only
 ip address 10.1.6.1 255.255.255.0
 dialer in-band
 dialer wait-for-carrier-time 60
 dialer string 0118527351234
 pulse-time 1
 dialer-group 1
!
interface Serial3
 description DDR interface to answer calls from remote office
 ip address 10.1.7.1 255.255.255.0
 dialer in-band
!
interface Serial4
 description configuration for PPP interface
 ip address 10.1.8.1 255.255.255.0
 encapsulation ppp
!
interface Serial5
 description Frame Relay configuration sample
 no ip address
 encapsulation frame-relay
!
interface Serial5.1 point-to-point
 description PVC to first office
 ip address 10.1.9.1 255.255.255.0
 frame-relay interface-dlci 16
!
interface Serial5.2 point-to-point
 description PVC to second office
 ip address 10.1.10.1 255.255.255.0
 frame-relay interface-dlci 17
!
interface Serial6
 description Configuration for PPP interface
 ip address 10.1.11.1 255.255.255.0
 encapsulation ppp
!
interface Serial7
 no ip address
 shutdown
!
interface Serial8
 ip address 10.1.12.1 255.255.255.0
 encapsulation ppp
 async default routing
 async mode dedicated
!
interface Serial9
 physical-layer async
 ip address 10.1.13.1 255.255.255.0
 encapsulation ppp
 async default routing
 async mode dedicated
!
```

```
interface Serial10
 physical-layer async
 no ip address
!
interface Serial11
 no ip address
 shutdown
!
interface Serial12
 physical-layer async
 no ip address
 shutdown
!
interface Serial13
 no ip address
 shutdown
!
interface Serial14
 no ip address
 shutdown
!
interface Serial15
 no ip address
 shutdown
!
interface Serial16
 no ip address
 shutdown
!
interface Serial17
 no ip address
 shutdown
```

Serial interface serial 18 is the first high-speed serial interface of the second 2T16S module. Remote sites on different subnets are dialing in to this interface with point-to-point and multipoint connections.

```
interface Serial18
 description Frame Relay sample
 no ip address
 encapsulation frame-relay
!
interface Serial18.1 point-to-point
 description Frame Relay subinterface
 ip address 10.1.14.1 255.255.255.0
 frame-relay interface-dlci 16
!
interface Serial18.2 point-to-point
 description Frame Relay subinterface
 ip address 10.1.15.1 255.255.255.0
 frame-relay interface-dlci 17
!
interface Serial18.3 point-to-point
 description Frame Relay subinterface
 ip address 10.1.16.1 255.255.255.0
 frame-relay interface-dlci 18
!
interface Serial18.5 multipoint
 ip address 10.1.17.1 255.255.255.0
 frame-relay map ip 10.1.17.2 100 IETF
```

This second high-speed serial interface is configured to connect a X.25 link. Serial interfaces 20 through 35 are the low-speed interfaces. However, some of the interfaces are not displayed in this example.

```
interface Serial19
 description X25 sample configuration
 ip address 10.1.18.1 255.255.255.0
 no ip mroute-cache
 encapsulation x25
 x25 address 6120000044
 x25 htc 25
 x25 map ip 10.1.18.2 6120170073
!
interface Serial20
 ip address 10.1.19.1 255.255.255.0
!
interface Serial21
 physical-layer async
 ip unnumbered e0
 encap ppp
 async mode dedicated
 async dynamic routing
 ipx network 45
 ipx watchdog-spoof
 dialer in-band
 dialer-group 1
 ppp authentication chap
!
interface Serial22
 no ip address
 shutdown
!
interface Serial23
 no ip address
 shutdown
!
interface Serial24
 no ip address
 shutdown
!
! Serial interfaces 23 through 35 would appear here.
.
.
.
 router eigrp 10
 network 10.0.0.0
!
 dialer-list 1 protocol ip permit
!
 line con 0
 exec-timeout 15 0
 password david
 login
```

The following basic line example configures some of the low-speed serial interfaces for the module:

```
line 8 10
 modem InOut
 transport input all
 rxspeed 64000
 txspeed 64000
 flowcontrol hardware
line 12
 transport input all
 rxspeed 64000
 txspeed 64000
 flowcontrol hardware
 modem chat-script generic
line 21
 transport input all
 rxspeed 64000
 txspeed 64000
 flowcontrol hardware
!
 end
```

Configuring Line Cards on the Cisco 7500 Series

This module describes software configuration commands needed to configure line cards with certain Cisco IOS software features for Cisco 7500 series routers.

Note On the Cisco 7507 and Cisco 7513 routers, you can install two Route Switch Processor (RSP) cards in a single router to improve system availability. This feature was introduced in Cisco IOS Release 11.1(4) as the "High System Availability (HSA)" feature. Because High Availability (HA) has since come to apply to a variety of Cisco IOS hardware and software features that allow for 99.9999% uptime for Cisco devices, this feature is now referred to as the "Dual RSP" feature.

Note Boot ROM revision 11.1(2) or higher is required for HSA to work with an RSP2 line card.

The boot ROM is on a SIMM on the RSP2 and cannot be upgraded. You can identify the boot ROM version on your RSP2 by issuing the **show version | begin ROM** command in privileged EXEC mode.

Performing a Single Line Card Reload

The **service single-slot-reload-enable** global configuration command allows you to enable the Single Line Card Reload feature, a High Availability (HA) feature for Cisco 7500 series routers. When this feature is enabled, if a single line card crashes, only the line card that failed is reloaded. The physical lines and the routing protocols on the other line cards remain active (note that some packets may be dropped while the card reloads, but only packets that depend on the crashed card will be affected).

A single line card reload is substantially faster than the Cbus Complex process used in some early Cisco IOS releases.

The Cisco 7500 Single Line Card Reload feature works on all RSP images.

Note The Single Line Card Reload feature is disabled by default. Enabling this feature is highly recommended.

Configuring Dual RSPs on Cisco 7500 Series Routers

To configure Dual RSP operation, you must have a Cisco 7507 or Cisco 7513 router containing two RSP processor cards. For Dual RSP compatibility, download a Cisco IOS software subset image that has a "v" in it. For example, rsp-jv-mz, rsp-ajv-mz, and rsp-pv-mz are all Dual RSP-compatible Cisco IOS subset images.

Two RSP cards in a router provide the most basic level of increased system availability through a "cold restart" feature. A "cold restart" means that when one RSP card fails, the other RSP card reboots the router. In this way, your router is never in a failed state for very long, thereby increasing system availability.

When one RSP card takes over operation from another, system operation is interrupted. This change is similar to issuing the **reload** EXEC command. The following events occur when one RSP card fails and the other takes over:

- The router stops passing traffic.
- Route information is lost.
- All connections are lost.
- The backup or "slave" RSP card becomes the active or "master" RSP card that reboots and runs the router. Thus, the slave has its own image and configuration file so that it can act as a single processor.

Note Having Dual RSPs does not impact performance in terms of packets per second or overall bandwidth. The Dual RSP feature does not provide fault-tolerance or redundancy.

Understanding Master and Slave Operation

A router configured for Dual RSP operation has one RSP card that is the master and one that is the slave. The master RSP card functions as if it were a single processor, controlling all functions of the router. The slave RSP card does nothing but actively monitor the master for failure.

A system crash can cause the master RSP to fail or go into a nonfunctional state. When the slave RSP detects a nonfunctional master, the slave resets itself and takes part in *master-slave arbitration*. Master-slave arbitration is a ROM monitor process that determines which RSP card is the master and which is the slave upon startup (or reboot).

If a system crash causes the master RSP to fail, the slave RSP becomes the new master RSP and uses its own system image and configuration file to reboot the router. The failed RSP card now becomes the slave. The failure state of the slave (formerly the master) can be accessed from the console via the **show stacks** EXEC command.

With Dual RSP operation, the following items are important to note:

- An RSP card that acts as the slave runs a different software version than it does when it acts as the master. The slave mode software is a subset of the master mode software.
- The two RSP cards need not run the same master software image and configuration file. When the slave reboots the system and becomes the new master, it uses its own system image and configuration file to reboot the router.
- When enabled, automatic synchronization mode automatically ensures that the master and slave RSP card have the same configuration file.

- Both hardware and software failures can cause the master RSP to enter a nonfunctional state, but the system does not indicate the type of failure.
- The console is always connected to master. A Y cable is shipped with your Cisco 7507 or Cisco 7513 router. The “top” of the Y cable plugs into the console port on each RSP card, and the “bottom” of the Y cable plugs into a terminal or terminal server. The master RSP card has ownership of the Y cable in that the slave Universal Asynchronous Receiver Transmitter (UART) drivers are disabled. Thus, no matter which RSP card is configured as the master, your view of the internetwork environment is always from the master’s perspective. Refer to your product’s hardware installation and maintenance publication for information on properly installing the Y cable.

Understanding Dual RSP Implementation Methods

There are two common ways to use the Dual RSP feature, as follows:

- Simple hardware backup. Use this method to protect against an RSP card failure. With this method, you configure both RSP cards with the same software image and configuration information. Also, you configure the router to automatically synchronize configuration information on both cards when changes occur.
- Software error protection. Use this method to protect against critical Cisco IOS software errors in a particular release. With this method, you configure the RSP cards with different software images, but with the same configuration information. If you are using new or experimental Cisco IOS software, consider using the software error protection method.

You can also use Dual RSPs for advanced implementations. For example, you can configure the RSP cards with the following implementations:

- Same software images but different configuration files
- Different software images and different configuration files
- Widely varied configuration files (for example, various features or interfaces can be turned off and on per card)

Note Although other uses are possible, the configuration information in this guide describes commands for only the two common methods—simple hardware backup and software error protection.

Dual RSP Configuration Task List

To configure Dual RSP operation, perform the tasks described in the following sections. The first two and last two tasks are required for both implementations. The third and fourth tasks relates to simple hardware backup. The fifth task relates to software error protection only.

- Specifying the Default Slave RSP (both implementations)
- Ensuring That Both RSP Cards Contain the Same Configuration File (both implementations)
- Ensuring That Both RSP Cards Contain the Same System Image (simple hardware backup only)
- Ensuring That Both RSP Cards Contain the Same Microcode Image (simple hardware backup only)
- Specifying Different Startup Images for the Master and Slave RSPs (software error protection only)
- Setting Environment Variables on the Master and Slave RSP (both implementations)
- Monitoring and Maintaining Dual RSP Operation (both implementations)

Specifying the Default Slave RSP

To specify the default slave RSP card, use the following command in global configuration mode:

Command	Purpose
Router(config)# **slave default-slot** *processor-slot-number*	Specifies the slave RSP card.

After specifying the default slave card, save the running configuration to the startup configuration using the **copy running-config startup-config** or **copy system:running-config nvram:startup-config** EXEC command. When the system is rebooted, the RSP specification will take effect (if both RSP cards are operational): The specified default slave becomes the slave RSP card and the other RSP card takes over as the master RSP card.

The router uses the default slave information when booting as follows:

- If a system boot is due to powering up the router or using the **reload** EXEC command, then the specified default slave will be the slave RSP.
- If a system boot is due to a system crash or hardware failure, then the system ignores the default slave designation and makes the crashed or faulty RSP the slave RSP.

If you do not specifically define the default slave RSP, the RSP card located in the higher number processor slot is the default slave. On the Cisco 7507 router, processor slot 3 contains the default slave RSP. On the Cisco 7513 router, processor slot 7 contains the default slave RSP.

The following example sets the default slave RSP to processor slot 2 on a Cisco 7507 router:

```
Router# configure terminal
Router (config)# slave default-slot 2
Router (config)# end
Router# copy system:running-config nvram:startup-config
```

Ensuring That Both RSP Cards Contain the Same Configuration File

With both the simple hardware backup and software error protection implementation methods, you always want your master and slave configuration files to match. To ensure that they match, turn on automatic synchronization. In automatic synchronization mode, the master copies its startup configuration to the slave’s startup configuration when you issue a **copy** EXEC command that specifies the master’s startup configuration (**nvram:startup-config**) as the target.

Automatic synchronization mode is on by default; in the event that you need to reenable the automatic synchronization, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router# **slave auto-sync config**	Reenables automatic synchronization mode.
Step 3	Router# **end**	Exits configuration mode.
Step 4	Router(config)# **copy system:running-config nvram:startup-config** or Router(config)# **copy running-config startup-config**	Saves this information to the system startup configuration and copies the configuration to the slave’s startup configuration.

Ensuring That Both RSP Cards Contain the Same System Image

For simple hardware backup, ensure that both RSP cards have the same system image.

To ensure that both RSP cards have the same system image, use the following commands in EXEC mode:

	Command	Purpose
Step 1	`Router#` **`show bootvar`**	Displays the contents of the BOOT environment variable to learn the current booting parameters for the master and slave RSP.
Step 2	Router# **dir** {**bootflash:** | **slot0:** | **slot1:**}	Verifies the location and version of the master RSP software image.
Step 3	Router# **dir** {**slavebootflash:** | **slaveslot0:** | **slaveslot1:**}	Determines if the slave RSP contains the same software image in the same location.
Step 4	Router# **copy** {**bootflash:**[*filename*] | **slot0:**[*filename*] | **slot1:**[*filename*]}{**slavebootflash:**[*filename*] | **slaveslot0:**[*filename*] | **slaveslot1:**[*filename*]}	If the slave RSP does not contain the same system image in the same location, copies the master's system image to the appropriate slave location. Note that you may also need to use the **delete** or **squeeze** EXEC command in conjunction with the **copy** command to accomplish this step.

The following example shows the process of ensuring that both RSP cards have the same system image. Note that because no environment variables are set, the default environment variables are in effect for both the master and slave RSP. Therefore, the router will boot the image in slot 0.

```
Router# show bootvar

BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
BOOTLDR variable does not exist

Configuration register is 0x0

current slave is in slot 7
BOOT variable =
CONFIG_FILE variable =
BOOTLDR variable does not exist

Configuration register is 0x0

Router# dir slot0:
-#- -length- -----date/time------ name
1    3482498  May 4 1993 21:38:04 rsp-k-mz11.2

7993896 bytes available (1496 bytes used)

Router# dir slaveslot0:
-#- -length- -----date/time------ name
1    3482498  May 4 1993 21:38:04 rsp-k-mz11.1

7993896 bytes available (1496 bytes used)

Router# delete slaveslot0:rsp-k-mz11.1
Router# copy slot0:rsp-k-mz11.2 slaveslot0:rsp-k-mz11.2
```

Ensuring That Both RSP Cards Contain the Same Microcode Image

To ensure that interface processors will load the same microcode, regardless of which RSP is used, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	`Router#` **`show controller cbus`**	Determines the microcode images used on the interface processors. If all interface processors are running from the bundled system microcode, no further action is required.
Step 2	`Router#` **`dir`** `{`**`bootflash:`** `|` **`slot0:`** `|` **`slot1:`**`}`	If any interface processors are running from the Flash file system, verifies the location and version of the master RSP's supplementary microcode.
Step 3	`Router#` **`dir`** `{`**`slavebootflash:`** `|` **`slaveslot0:`** `|` **`slaveslot1:`**`}`	Determines if the slave RSP contains the same microcode image in the same location.
Step 4	`Router#` **`copy`** `{`**`bootflash:`**`[`*`filename`*`]` `|` **`slot0:`**`[`*`filename`*`]` `|` **`slot1:`**`[`*`filename`*`]}` `{`**`slavebootflash:`**`[`*`filename`*`]` `|` **`slaveslot0:`**`[`*`filename`*`]` `|` **`slaveslot1:`**`[`*`filename`*`]}`	If the slave RSP does not contain the same microcode image in the same location, copies the master's microcode image to the appropriate slave location. Note that you also may need to use the **delete** or **squeeze** command in conjunction with the **copy** command to accomplish this step.

The following example ensures that both RSP cards have the same microcode image. Notice that slots 0, 1, 4, 9, and 10 load microcode from the bundled software, as noted by the statement "software loaded from system." Slot 11, the Fast Serial Interface Processor (FSIP), does not use the microcode bundled with the system. Instead, it loads the microcode from slot0:pond/bath/rsp_fsip20-1. Thus, you must ensure that the slave RSP has a copy of the same FSIP microcode in the same location.

```
Router# show controller cbus

MEMD at 40000000, 2097152 bytes (unused 416, recarves 3, lost 0)
  RawQ 48000100, ReturnQ 48000108, EventQ 48000110
  BufhdrQ 48000128 (2948 items), LovltrQ 48000140 (5 items, 1632 bytes)
  IpcbufQ 48000148 (16 items, 4096 bytes)
  3571 buffer headers (48002000 - 4800FF20)
  pool0: 28 buffers, 256 bytes, queue 48000130
  pool1: 237 buffers, 1536 bytes, queue 48000138
  pool2: 333 buffers, 4544 bytes, queue 48000150
  pool3: 4 buffers, 4576 bytes, queue 48000158
  slot0: EIP, hw 1.5, sw 20.00, ccb 5800FF30, cmdq 48000080, vps 4096
    software loaded from system
    Ethernet0/0, addr 0000.0ca3.cc00 (bia 0000.0ca3.cc00)
      gfreeq 48000138, lfreeq 48000160 (1536 bytes), throttled 0
      rxlo 4, rxhi 42, rxcurr 0, maxrxcurr 2
      txq 48000168, txacc 48000082 (value 27), txlimit 27
                  .........
slot1: FIP, hw 2.9, sw 20.02, ccb 5800FF40, cmdq 48000088, vps 4096
    software loaded from system
    Fddi1/0, addr 0000.0ca3.cc20 (bia 0000.0ca3.cc20)
      gfreeq 48000150, lfreeq 480001C0 (4544 bytes), throttled 0
      rxlo 4, rxhi 165, rxcurr 0, maxrxcurr 0
      txq 480001C8, txacc 480000B2 (value 0), txlimit 95
 slot4: AIP, hw 1.3, sw 20.02, ccb 5800FF70, cmdq 480000A0, vps 8192
    software loaded from system
    ATM4/0, applique is SONET (155Mbps)
      gfreeq 48000150, lfreeq 480001D0 (4544 bytes), throttled 0
      rxlo 4, rxhi 165, rxcurr 0, maxrxcurr 0
      txq 480001D8, txacc 480000BA (value 0), txlimit 95
 slot9: MIP, hw 1.0, sw 20.02, ccb 5800FFC0, cmdq 480000C8, vps 8192
    software loaded from system
    T1 9/0, applique is Channelized T1
      gfreeq 48000138, lfreeq 480001E0 (1536 bytes), throttled 0
      rxlo 4, rxhi 42, rxcurr 0, maxrxcurr 0
      txq 480001E8, txacc 480000C2 (value 27), txlimit 27
                .......

 slot10: TRIP, hw 1.1, sw 20.00, ccb 5800FFD0, cmdq 480000D0, vps 4096
    software loaded from system
    TokenRing10/0, addr 0000.0ca3.cd40 (bia 0000.0ca3.cd40)
      gfreeq 48000150, lfreeq 48000200 (4544 bytes), throttled 0
      rxlo 4, rxhi 165, rxcurr 1, maxrxcurr 1
      txq 48000208, txacc 480000D2 (value 95), txlimit 95
               .........

 slot11: FSIP, hw 1.1, sw 20.01, ccb 5800FFE0, cmdq 480000D8, vps 8192
    software loaded from flash slot0:pond/bath/rsp_fsip20-1
    Serial11/0, applique is Universal (cable unattached)
      gfreeq 48000138, lfreeq 48000240 (1536 bytes), throttled 0
      rxlo 4, rxhi 42, rxcurr 0, maxrxcurr 0
      txq 48000248, txacc 480000F2 (value 5), txlimit 27
              ...........

Router# dir slot0:pond/bath/rsp_fsip20-1
-#- -length- -----date/time------ name
3   10242    Jan 01 1995 03:46:31 pond/bath/rsp_fsip20-1

Router# dir slaveslot0:pond/bath/rsp_fsip20-1
No such file

4079832 bytes available (3915560 bytes used)

Router# copy slot0:pond/bath/rsp_fsip20-1 slaveslot0:
4079704 bytes available on device slaveslot0, proceed? [confirm]

Router# dir slaveslot0:pond/bath/rsp_fsip20-1
-#- -length- -----date/time------ name
3   10242    Mar 01 1993 02:35:04 pond/bath/rsp_fsip20-1

4069460 bytes available (3925932 bytes used)
```

Specifying Different Startup Images for the Master and Slave RSPs

For software error protection, the RSP cards should have different system images.

When the factory sends you a new Cisco 7507 or Cisco 7513 router with two RSPs, you receive the same system image on both RSP cards. For the software error protection method, you need two different software images on the RSP cards. Thus, you copy a desired image to the master RSP card and modify the **boot system** global configuration commands to reflect booting two different system images. Each RSP card uses its own image to boot the router when it becomes the master.

To specify different startup images for the master and slave RSP, use the following commands beginning in EXEC mode:

	Command	Purpose
Step 1	Router# **dir** {**bootflash:** | **slot0:** | **slot1:**}	Verifies the location and version of the master RSP software image.
Step 2	Router# **dir** {**slavebootflash:** | **slaveslot0:** | **slaveslot1:**}	Determines if the slave RSP contains the same software image in the same location.
Step 3	Router# **copy** *source-url* {**bootflash:** | **slot0:** | **slot1:**}	Copies a different system image to the master RSP.
Step 4	Router# **configure terminal**	Enters configuration mode from the terminal.
Step 5	Router(config)# **boot system flash bootflash:**[*filename*] Router(config)# **boot system flash slot0:**[*filename*] Router(config)# **boot system flash slot1:**[*filename*]	From global configuration mode, configures the master RSP to boot the new image from the appropriate location.
Step 6	Router(config)# **boot system flash** Router(config)# **bootflash:**[*filename*] Router(config)# **boot system flash slot0:**[*filename*] Router(config)# **boot system flash slot1:**[*filename*]	Also, add a **boot system** command that specifies the slave's boot image and location. This is the boot image that the slave uses when it becomes the master RSP and boots the system. Note that because the slave will boot this image when the slave is actually the new master RSP, the command syntax does not use a "**slave**" prefix.
Step 7	Router(config)# **boot system** {**rcp** | **tftp** | **ftp**} [*filename*] [*ip-address*]	(Optional) Configures the master RSP to boot from a network server.
Step 8	Router(config)# **config-register** *value*	Sets the configuration register to enable the system to load the system image from a network server or from Flash.
Step 9	Router(config)# **end**	Exits configuration mode.
Step 10	Router# **copy system:running-config nvram:startup-config** OR Router# **copy running-config startup-config**	Saves the configuration file to the master's startup configuration. Because automatic synchronization is turned on, this step saves the **boot system** commands to the master and slave startup configuration.
Step 11	Router# **reload**	Resets the router with the new configuration information.

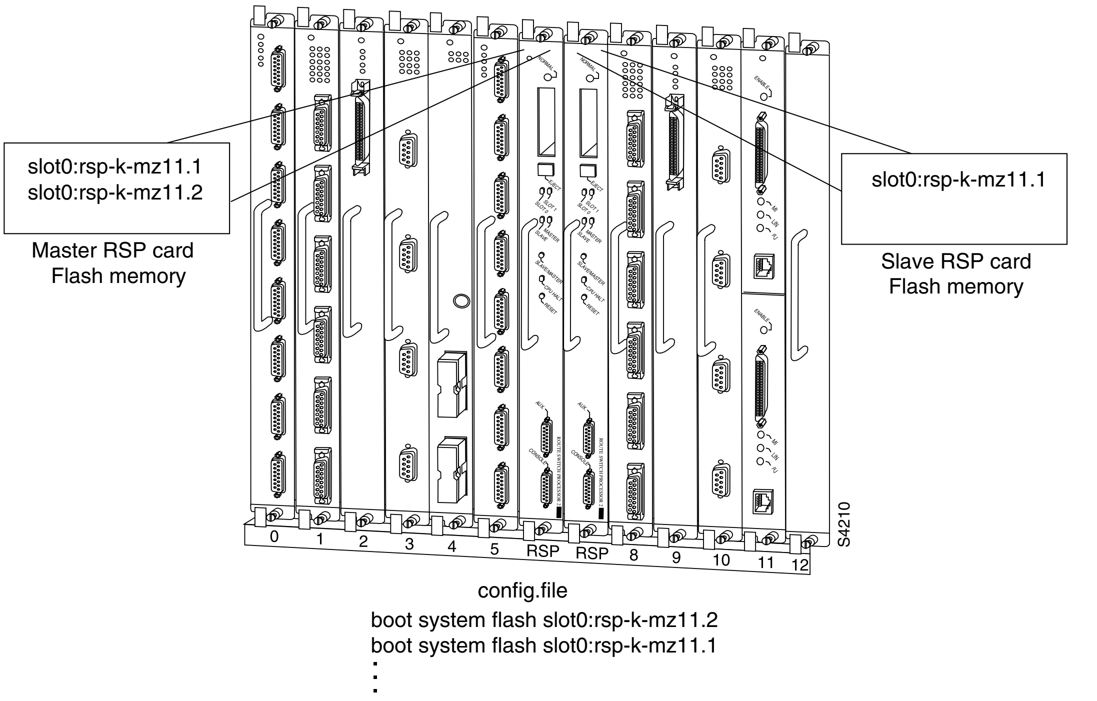
Upgrading to a New Software Version Example

In this example, assume the following:

- The master RSP is in processor slot 6 and the slave RSP is in processor slot 7 of a Cisco 7513 router.
- The system has the same image rsp-k-mz11.1 in PCMCIA slot 0 of both the master and slave RSP card.
- You want to upgrade to Cisco IOS Release 12.0, but you want to guard against software failures. So, you configure Dual RSP operation for software error protection.

Figure 36 illustrates the software error protection configuration for this example. The configuration commands for this configuration follow the figure.

Figure 36 Software Error Protection: Upgrading to a New Software Version



Because you always view the environment from the master RSP perspective, in the following command you view the master's slot 0 to verify the location and version of the master's software image:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1    3482496  May 4 1993 21:38:04 rsp-k-mz11.1

7993896 bytes available (1496 bytes used)
```

Now view the slave's software image location and version:

```
Router# dir slaveslot0:
-#- -length- -----date/time------ name
1    3482496  May 4 1993 21:38:04 rsp-k-mz11.1

7993896 bytes available (1496 bytes used)
```

Because you want to run the Release 12.0 system image on one RSP card and the Release 11.1 system image on the other RSP card, copy the Release 12.0 system image to the master's slot 0:

```
Router# copy tftp: slot0:rsp-k-mz12.0
```

Enter global configuration mode and configure the system to boot first from a Release 12.0 system image and then from a Release 11.1 system image:

```
Router# configure terminal
Router (config)# boot system flash slot0:rsp-k-mz12.0
Router (config)# boot system flash slot0:rsp-k-mz11.1
```

With this configuration, when the slot 6 RSP card is master, it looks first in its PCMCIA slot 0 for the system image file rsp-k-mz11.2 to boot. Finding this file, the router boots from that system image. When the slot 7 RSP card is master, it also looks first in its slot 0 for the system image file rsp-k-mz12.0 to boot. Because that image does not exist in that location, the slot 7 RSP card looks for the system image file rsp-k-mz11.1 in slot 0 to boot. Finding this file in its PCMCIA slot 0, the router boots from that system image. In this way, each RSP card can reboot the system using its own system image when it becomes the master RSP card.

Configure the system further with a fault-tolerant booting strategy:

```
Router (config)# boot system tftp rsp-k-mz11.1 192.168.1.25
```

Set the configuration register to enable loading of the system image from a network server or from Flash and save the changes to the master and slave startup configuration file:

```
Router (config)# config-register 0x010F
Router (config)# end
Router# copy system:running-config nvram:startup-config
```

Reload the system so that the master RSP uses the new Release 12.0 system image:

```
Router# reload
```

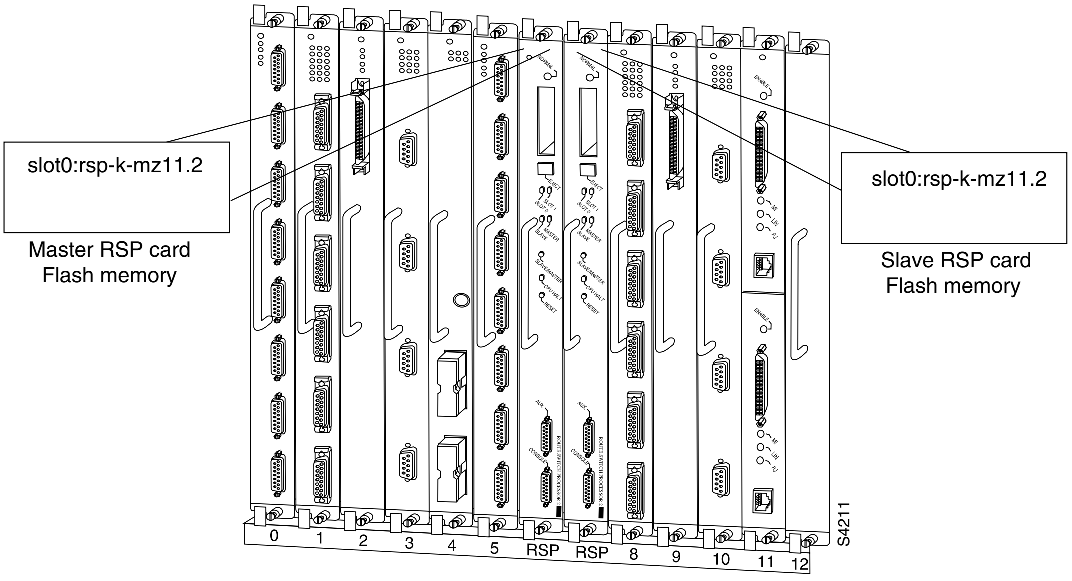
Dual RSP: Backing Up with an Older Software Version Example

In the following example, assume the following:

- The master RSP is in processor slot 6 and the slave RSP is in processor slot 7 of a Cisco 7513 router.
- The system has the same image rsp-k-mz11.2 in PCMCIA slot 0 of both the master and slave RSP card.
- You want to use to Cisco IOS Release 11.1 as backup to guard against software failures. So, you configure Dual RSP operation for software error protection.

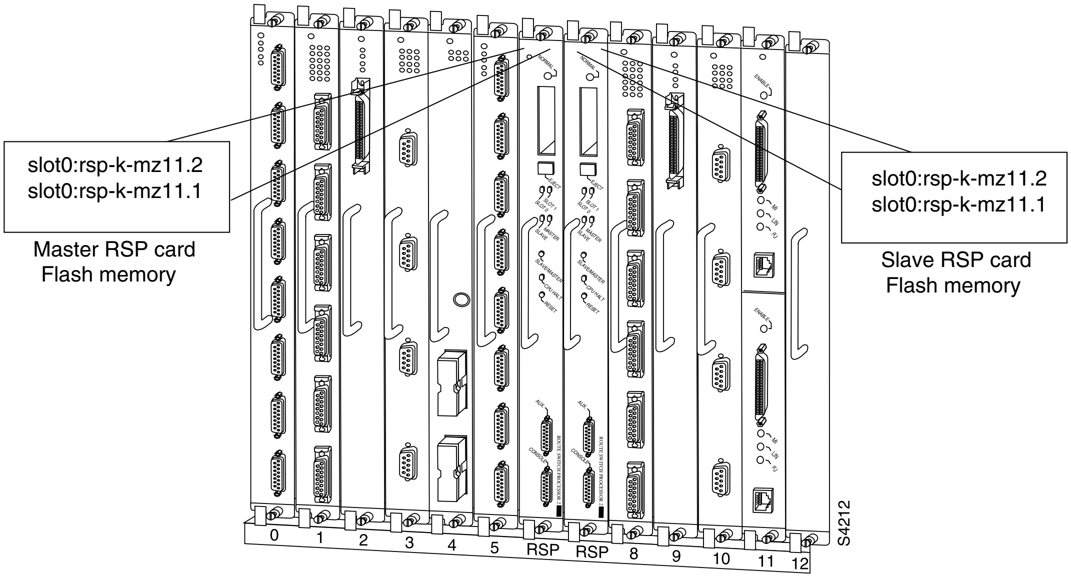
In this scenario, you begin with the configuration shown in Figure 37.

Figure 37 Software Error Protection: Backing Up with an Older Software Version, Part I



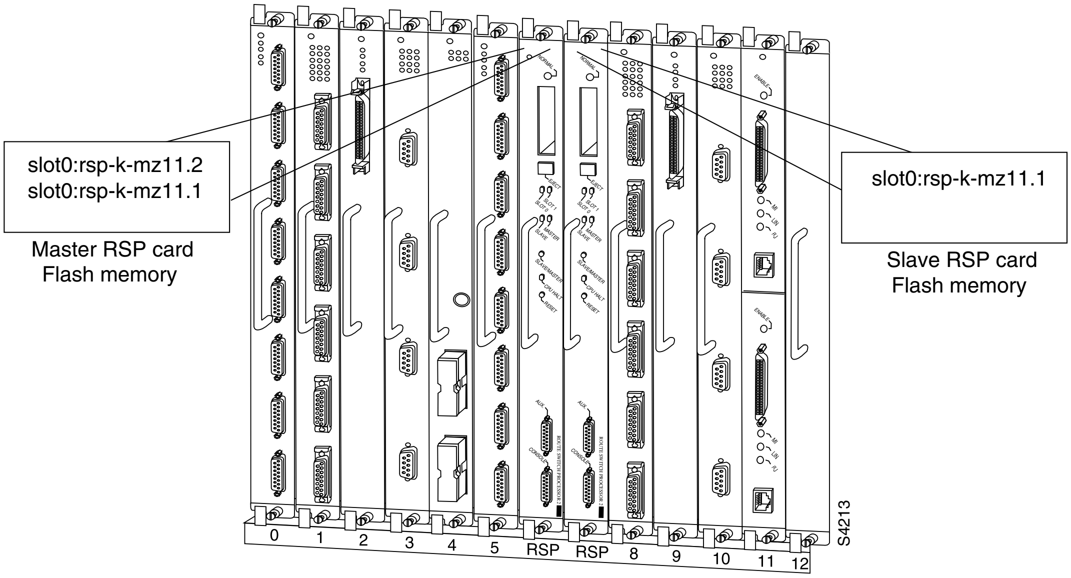
First, copy the rsp-k-mz11.1 image to the master and slave RSP card, as shown in Figure 38.

Figure 38 Software Error Protection: Backing Up with an Older Software Version, Part 2



Next, you delete the rsp-k-mz11.2 image from the slave RSP card. The final configuration is shown in Figure 39.

Figure 39 Software Error Protection: Backing Up with an Older Software Version, Part 3



The following commands configure software error protection for this example scenario.

View the master and slave slot 0 to verify the location and version of their software images:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1    3482498  May 4 1993 21:38:04 rsp-k-mz11.2
```

```
7993896 bytes available (1496 bytes used)

Router# dir slaveslot0:
-#- -length- -----date/time------ name
1    3482498  May 4 1993 21:38:04 rsp-k-mz11.2

7993896 bytes available (1496 bytes used)
```

Copy the Release 11.1 system image to the master and slave slot 0:

```
Router# copy tftp: slot0:rsp-k-mz11.1
Router# copy tftp: slaveslot0:rsp-k-mz11.1
```

Delete the rsp-k-mz11.2 image from the slave RSP card:

```
Router# delete slaveslot0:rsp-k-mz11.2
```

Configure the system to boot first from a Release 11.2 system image and then from a Release 11.1 system image:

```
Router# configure terminal
Router (config)# boot system flash slot0:rsp-k-mz11.2
Router (config)# boot system flash slot0:rsp-k-mz11.1
```

Configure the system further with a fault-tolerant booting strategy:

```
Router (config)# boot system tftp rsp-k-mz11.1 192.168.1.25
```

Set the configuration register to enable loading of the system image from a network server or from Flash and save the changes to the master and slave startup configuration file:

```
Router (config)# config-register 0x010F
Router (config)# end
Router# copy system:running-config nvram:startup-config
```

Note You do not need to reload the router in this example, because the router is currently running the Release 11.2 image.

Setting Environment Variables on the Master and Slave RSP

You can set environment variables on both RSP cards in a Cisco 7507 and Cisco 7513 router.

Note When you configure Dual RSP operation, we recommend that you use the default environment variables. If you change the variables, we recommend setting the same device for equivalent environment variables on each RSP card. For example, if you set one RSP card’s CONFIG_FILE environment variable device to NVRAM, set the other RSP card’s CONFIG_FILE environment variable device to NVRAM as well.

You set environment variables on the master RSP just as you would if it were the only RSP card in the system. See the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 for more information on the following steps:

- Specifying the Startup System Image in the Configuration File (in the “Loading and Maintaining System Images” chapter).
- Controlling Environment Variables (in the “Rebooting” chapter).

You can set the same environment variables on the slave RSP card, manually or automatically. The following sections describe these two methods:

- Automatically Setting Environment Variables on the Slave RSP
- Manually Setting Environment Variables on the Slave RSP

Automatically Setting Environment Variables on the Slave RSP

With automatic synchronization turned on, the system automatically saves the same environment variables to the slave's startup configuration when you set the master's environment variables and save them.

Note Automatic synchronization mode is on by default. To turn off automatic synchronization, use the **no slave auto-sync config** global configuration command.

To set environment variables on the slave RSP when automatic synchronization is on, set the environment variables as described in the "Rebooting" chapter of the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4. You can verify the boot variable using the **show bootvar** EXEC mode command.

Manually Setting Environment Variables on the Slave RSP

If you disable automatic synchronization of configuration files, you must manually synchronize the slave's configuration file to the master's configuration file to store environment variables on the slave RSP.

Once you set the master's environment variables, you can manually set the same environment variables on the slave RSP card using the **slave sync config** EXEC command.

To manually set environment variables on the slave RSP, perform the following procedure:

Step 1 Set the environment variables for the master RSP card as described in the "Rebooting" chapter of the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4.

Step 2 Save the configuration using the **copy system:running-config nvram:startup-config** EXEC command.

Step 3 Save the same environment variable configuration to the slave RSP using the **slave sync config** privileged EXEC command. Issuing this command will synchronize the configuration files.

Step 4 Verify the environment variable settings using the **show bootvar** EXEC command.

Monitoring and Maintaining Dual RSP Operation

To monitor and maintain Dual RSP operation, complete the following tasks in the following sections:

- Overriding the Slave Image Bundled with the Master Image
- Manually Synchronizing Configuration Files
- Troubleshooting and Reloading a Failed RSP Card

- Disabling Access to the Slave Console
- Displaying Information About Master and Slave RSP Cards

Overriding the Slave Image Bundled with the Master Image

To override the slave image that is bundled with the master image, use the following command in global configuration mode:

Command	Purpose
`Router(config)# slave image {system	file-url}`	Specifies which image the slave runs.

Manually Synchronizing Configuration Files

To manually synchronize configuration files and ROM monitor environment variables on the master and slave RSP card, use the following command in privileged EXEC mode:

Command	Purpose
`Router(config)# slave sync config`	Manually synchronizes the master and slave configuration files.

Caution When you install a second RSP card for the first time, you *must* immediately configure it using the **slave sync config** command. This ensures that the new slave is configured consistently with the master. Failure to do so can result in an unconfigured slave RSP card taking over mastership of the router when the master fails, potentially rendering the network inoperable.

The **slave sync config** command is also a useful tool for more advanced implementation methods not discussed in this chapter.

Troubleshooting and Reloading a Failed RSP Card

When a new master RSP card takes over mastership of the router, it automatically reboots the failed RSP card as the slave RSP card. You can access the state of the failed RSP card in the form of a stack trace from the master console using the **show stacks** EXEC command.

The **debug oir** command is used to debug the online insertion and removal (OIR) feature (which is also known as hot-swapping or power-on servicing). The **debug oir** command often is useful in debugging problems related to OIR, including single line card reloading.

You can also manually reload a failed, inactive RSP card from the master console. This task returns the card to the active slave state. If the master RSP fails, the slave will be able to become the master. To manually reload the inactive RSP card, use the following command in global configuration mode:

Command	Purpose
`Router(config)# slave reload`	Reloads the inactive slave RSP card.

Disabling Access to the Slave Console

The slave console does not have enable password protection. Thus, a user connected to the slave console port can enter privileged EXEC mode and view or erase the configuration of the router. Use the **no slave terminal** global configuration command to disable slave console access and prevent security problems. When the slave console is disabled, users cannot enter commands.

If slave console access is disabled, the following message appears periodically on the slave console:

```
%%Slave terminal access is disabled. Use "slave terminal" command in master RSP
configuration mode to enable it.
```

Displaying Information About Master and Slave RSP Cards

To display information about both the master and slave RSP cards, use the following commands in EXEC mode, as needed:

Command	Purpose
`Router# show bootvar`	Displays the environment variable settings and configuration register settings for both the master and slave RSP cards.
`Router# show file systems`	Displays a list of Flash devices currently supported on the router.
`Router# show version`	Displays the software version running on the master and slave RSP card.
`Router# show stacks`	Displays the stack trace and version information of the master and slave RSP cards.

Clear Channel T3/E3 with Integrated CSU/DSU

The Clear Channel T3/E3 NM-1 Network Module with Integrated CSU/DSU feature provides a software configurable T3/E3 product. This flexible network module allows you to switch between T3 and E3 applications with a single Cisco IOS command.

The T3/E3 NM-1 network module supports a single-port T3 or E3 with an integrated channel service unit (CSU) and a data service unit (DSU). It supports High-Level Data Link Control (HDLC), PPP, and Frame Relay. It includes the following features:

- Single port—universal T3/E3 version
- Clear and subrate support on both T3 and E3 modes
- Online insertion and removal (OIR) support on Cisco 3660 series and Cisco 3745 routers
- Onboard processing of Cisco Message Definition Language (MDL) and performance monitoring
- Support for scrambling and subrate can be independently or simultaneously enabled in each DSU mode
- Support for full T3 and E3 line rates

T3/E3 Applications and Positioning

The T3/E3 NM-1 network module provides high-speed performance for advanced, fully converged networks supporting a wide array of applications and services such as security and advanced QoS for voice and video. T3/E3 and subrate T3/E3 connectivity optimizes WAN bandwidth for deploying the new applications and service delivery. All the supported platforms, except the Cisco 2650XM or Cisco 2651XM routers, are capable of supporting line rate performance but impose varying levels of CPU overhead and therefore affect the overall platform performance. See Table 24 for recommended branch office positioning.

Table 24 T3/E3 NM-1 Branch Office Positioning and Support Comparison

Supported Platforms	Recommended Type of Service	Recommended Branch Office Sizes	Maximum T3/E3 Modes Supported
Cisco 2650/2651XM	Subrate T3/E3	Small to medium offices	1 [1]
Cisco 2691	Subrate T3/E3	Small to medium offices	1
Cisco 3660 series	Subrate and full-rate T3/E3	Large and regional offices	1
Cisco 3725	Subrate and full-rate T3/E3	Medium and large offices	1
Cisco 3745	Subrate and full-rate T3/E3	Medium, large, and regional offices	2

1. For Cisco 2650XM and Cisco 2651XM platforms only, we recommend that you configure the NM-1 T3/E3 in subrate mode with a DSU setting of 15000 (15 mbps). All other platforms can operate with full DSU bandwidth.

Feature Specifications for the Clear Channel T3/E3 with Integrated CSU/DSU Feature

Feature History	
Release	**Modification**
12.2(11)YT	This feature was introduced.
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T.
Supported Platforms	
Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and 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

Prerequisites for Clear Channel T3/E3 with Integrated CSU/DSU

- Implementation of this feature requires Cisco IOS Release 12.2(11)YT or a later release.
- See Table 25 for the minimum platform memory recommended.

Table 25 Minimum Memory Requirements

Supported Platforms	Flash Memory	DRAM Memory
Cisco 2650/2651XM	8 MB	32 MB
Cisco 2691	32 MB	64 MB
Cisco 3660 series	8 MB	64 MB

Table 25 Minimum Memory Requirements

Supported Platforms	Flash Memory	DRAM Memory
Cisco 3725	32 MB	128 MB
Cisco 3745	32 MB	128 MB

Information About Clear Channel T3/E3 with Integrated CSU/DSU

Configuration of the Clear Channel T3/E3 with Integrated CSU/DSU feature can be set up for a T3 interface and for an E3 interface:

- How to Configure the Clear Channel T3/E3 with Integrated CSU/DSU Feature for a T3 Interface, page 341
- How to Configure the Clear Channel T3/E3 with Integrated CSU/DSU Feature for an E3 Interface, page 349

How to Configure the Clear Channel T3/E3 with Integrated CSU/DSU Feature for a T3 Interface

This section describes the tasks used to configure the Clear Channel T3/E3 with Integrated CSU/DSU feature for a T3 interface:

- Configuring the Card Type and Controller for a T3 Interface (required)
- Configuring DSU Mode and Bandwidth for T3 (required)
- Configuring Scrambling for T3 (optional)
- Configuring the BERT for T3 (optional)
- Configuring Loopback for T3 (optional)
- Configuring the T3 Maintenance Data Link (optional)

Configuring the Card Type and Controller for a T3 Interface

When the Clear Channel T3/E3 network module is used for the first time, the running configuration does not show the T3/E3 controller and its associated serial interface. You can use the **show version** command to learn if the router recognized the T3/E3 card and was able to initialize the card properly. After the card type is configured for the slot, the respective controller and serial interface appear in the running configuration. See the "Use the show version Command" section on page 357.

After the network module has ascertained that the card has been initialized properly, use the **card type** command to configure the card. If the command is accepted successfully, Cisco IOS software creates a controller and a serial interface for the card.

Perform this task to select and configure a card type and controller as T3.

Note The autoconfig/setup utility does not support configuring the card type for the T3/E3 network module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **card type t3** *slot*
4. **controller t3** *slot***/***port*
5. **framing** {**c-bit** | **m23**}
6. **cablelength** *feet*
7. **clock source** {**internal** | **line**}
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**card type t3** *slot* **Example:** `Router(config)# card type t3 1`	Selects the card type. • Creates a T3 controller and a serial interface. • **t3**—Selects the T3 controller. • *slot*—Slot number of the interface. • By default, the T3 controller does not show up in the **show running-config** output.
Step 4	**controller t3** *slot***/***port* **Example:** `Router(config)# controller t3 1`	Specifies the T3 controller and enters controller configuration mode. • *slot***/***port*—Backplane slot number and port number on the controller.

Step 5	**framing** {**c-bit** | **m23**}
	Example:
	`Router(config-controller)# framing c-bit`
		Specifies the framing type.
		• **c-bit**—Specifies C-bit framing as the T3 framing type.
		• **m23**—Specifies M23 framing as the T3 framing type.

Step 6	**cablelength** *feet* **Example:** `Router(config-controller)# cablelength 250`	Specifies the distance from the routers to the network equipment. • *feet*—Number of feet in the range from 0 to 450. • The default value is 224 feet.

	Command or Action	Purpose

Step 7	**clock source** {**internal** | **line**}
	Example:
	`Router(config-controller)# clock source line`
		Selects the clock source.
		• **internal**—Specifies that the internal clock source is used. This is the default for T3.
		• **line**—Specifies that the network clock source is used. This is the default for E3.

Step 8	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration mode and returns to privileged EXEC mode.

Configuring DSU Mode and Bandwidth for T3

Perform this task to specify the interoperability mode and maximum allowable bandwidth used by a T3 controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial** *slot*/*port*
4. **dsu mode** {**0** | **1** | **2** | **3** | **4**}
5. **dsu bandwidth** *kbps*
6. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface serial** *slot*/*port* **Example:** `Router(config)# interface serial 1/1`	Specifies the serial interface created on the controller.

	Command	Purpose

Step 4	**dsu mode** {**0** | **1** | **2** | **3** | **4**}
	Example:
	`Router(config-if)# dsu mode 0`
		Specifies the interoperability mode used by a T3 controller.
		• **0**—Connects a T3 controller to another T3 controller or to a Digital Link DSU (DL3100). Bandwidth range is from 300 to 44210 kbps. This is the default.
		• **1**—Connects a T3 controller to a Kentrox DSU. Bandwidth range is from 1500 to 35000/44210 kbps.
		Note If the bandwidth is set to greater than 35000 kbps, it defaults to 44210 kbps.
		• **2**—Connects a T3 controller to a Larscom DSU. Bandwidth range is from 3100 to 44210 kbps.
		• **3**—Connects a T3 controller to an Adtran T3SU 300. Bandwidth range is from 75 to 44210 kbps.
		• **4**—Connects a T3 controller to a Verilink HDM 2182. Bandwidth range is from 1500 to 44210 kbps.

Step 5	**dsu bandwidth** *kbps* **Example:** `Router(config-if)# dsu bandwidth 44210`	Specifies the maximum allowable bandwidth in the range from 1 to 44210 kbps. • The real (actual) vendor-supported bandwidth is in the range from 75 to 44210 kbps. **Note** For the Cisco 2650XM and Cisco 2651XM platforms only, we recommend that you set the DSU bandwidth to 15000 in any subrate mode.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Scrambling for T3

Perform this task to enable encryption of the payload on the T3 controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial** *slot*/*port*
4. **scramble**
5. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface serial`** *`slot`***`/`***`port`*
	Example:
	`Router(config)# interface serial 1/1`
		Enters interface configuration mode.

Step 4	**`scramble`**
	Example:
	`Router(config-if)# scramble`
		Enables the scrambling of the payload.
		• Default is off.

Step 5	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the BERT for T3

Perform this task to configure a bit error rate (BER) test pattern on a T3 controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t3** *slot***/***port*
4. **bert pattern** {**2^23** | **2^20** | **2^15** | **1s** | **0s** | **alt-0-1**} **interval** *time*
5. **no bert**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`controller t3`** *`slot`***`/`***`port`*
	Example:
	`Router(config)# controller t3 1/1`
		Selects the T3 controller and enters controller configuration mode.
		• *slot*/*port*—Backplane slot number and port number on the controller.

Step 4	**`bert pattern`** `{`**`2^23`** `|` **`2^20`** `|` **`2^15`** `|` **`1s`** `|` **`0s`** `|` **`alt-0-1`**`}` **`interval`** *`time`*
	Example:
	`Router(config-controller)# bert pattern 2^20 interval 10000`
		Configures a bit error rate test pattern.
		• Acceptable values are:
		– **2^23**—Pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
		– **2^20**—Pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
		– **2^15**—Pseudorandom 0.151 test pattern that is 32,768 bits in length.
		– **1s**—Repeating pattern of ones (...111...).
		– **0s**—Repeating pattern of zeros (...000...).
		– **alt-0-1**—Repeating pattern of alternating zeros and ones (...01010...).
		• **interval** *time*—Specifies the duration of the BER test. The interval can be a value from 1 to 14,400 minutes.

Step 5	**`no bert`**
	Example:
	`Router(config-controller)# no bert`
		Disables the BERT test pattern.

Step 6	**`exit`**
	Example:
	`Router(config-controller)# exit`
		Exits controller configuration mode and returns to privileged EXEC mode.

Configuring Loopback for T3

Perform this task to loop an entire T3 line toward the line and back toward the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t3** *slot*/*port*
4. **loopback** {**local** | **network** {**line** | **payload**} | **remote**}
5. **no loopback**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`controller t3`** *`slot`*/*`port`*
	Example:
	`Router(config)# controller t3 1/1`
		Selects the T3 controller and enters controller configuration mode.
		• *slot*/*port*—Backplane slot number and port number on the controller.

Step 4	**`loopback`** {**`local`** | **`network`** {**`line`** | **`payload`**} | **`remote`**}
	Example:
	`Router(config-controller)# loopback local`
		Loops the T3 line toward the line and back toward the router,
		• **local**—Loops the data back toward the router and sends an AIS signal out toward the network. On a dual port card, it is possible to run channelized on one port and primary rate on the other port.
		• **network** {**line** | **payload**}—Sets the loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**).
		• **remote**—Sends a far-end alarm control (FEAC) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. M23 format does not support remote loopbacks.

	Command	Purpose

Step 5	`no loopback`
	Example:
	`Router(config-controller)# no loopback`
		Removes the loop.

Step 6	`exit`
	Example:
	`Router(config-controller)# exit`
		Exits controller configuration mode and returns to privileged EXEC mode.

Configuring the T3 Maintenance Data Link

Perform this task to configure the MDL message.

Note This configuration information is applicable only to C-bit parity T3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t3** *slot*/*port*
4. **mdl** {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} *string*}
5. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`controller t3 slot/port`
	Example:
	`Router(config)# controller t3 1/1`
		Selects the T3 controller and enters controller configuration mode.
		• *slot*/*port*—Backplane slot number and port number on the controller.

	Command	Purpose

Step 4	**mdl** {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} *string*}
	Example:
	`Router(config-controller)# mdl transmit path`
		Configures the MDL message.
		• **transmit path**—Enables transmission of the MDL Path message.
		• **transmit idle-signal**—Enables transmission of the MDL idle signal message.
		• **transmit test-signal**—Enables transmission of the MDL test signal message.
		• **string eic** *string*—Specifies the equipment identification code (EIC); can be up to 10 characters.
		• **string lic** *string*—Specifies the location identification code (LIC); can be up to 11 characters.
		• **string fic** *string*—Specifies the frame identification code (FIC); can be up to 10 characters.
		• **string unit** *string*—Specifies the unit identification code (UIC); can be up to 6 characters.
		• **string pfi** *string*—Specifies the facility identification code (PFI) sent in the MDL path message; can be up to 38 characters.
		• **string port** *string*—Specifies the port number string sent in the MDL idle signal message; can be up to 38 characters.
		• **string generator** *string*—Specifies the generator number string sent in the MDL test signal message; can be up to 38 characters.

Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration mode and returns to privileged EXEC mode.

How to Configure the Clear Channel T3/E3 with Integrated CSU/DSU Feature for an E3 Interface

The section describes the commands used to configure the Clear Channel T3/E3 with Integrated CSU/DSU feature for an E3 interface:

- Configuring the Card Type and Controller for an E3 Interface (required)
- Configuring Scrambling for E3 (required)
- Configuring the BERT for E3 (optional)
- Configuring Loopback for E3 (optional)
- Configuring National Bit for E3 (optional)

Configuring the Card Type and Controller for an E3 Interface

Perform this task to configure the card type and controller for a E3 interface.

Note The autoconfig/setup utility does not support configuring the card type for the T3/E3 network module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **card type e3** *slot*
4. **controller e3** *slot***/***port*
5. **framing** {**bypass** | **g751**}
6. **clock source** {**internal** | **line**}
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`card type e3`** *`slot`*
	Example:
	`Router(config)# card type e3 1`
		Selects the card type.
		• Creates an E3 controller and a serial interface.
		• **e3**—Specifies the E3 transmission scheme predominantly used in Europe.
		• Provides 34010 kbps.
		• *slot*—Slot number of the interface.
		• By default, the E3 controller does not show up in the **show running config** output.

Step 4	**`controller e3`** *`slot/port`*
	Example:
	`Router(config)# controller e3 1`
		Specifies the E3 controller and enters controller configuration mode.
		• *slot***/***port*—Backplane slot number and port number on the controller.

	Command or Action	Purpose

Step 5	**framing** {**bypass** | **g751**}
	Example:
	`Router(config-controller)# framing bypass`
		Specifies the framing type.
		• **bypass**—Specifies that the G.751 framing be bypassed.
		• **g751**—Specifies G.751 as the E3 framing type.
		• Default is **g751**.

Step 6	**clock source** {**internal** | **line**}
	Example:
	`Router(config-controller)# clock source line`
		Selects the clock source.
		• **internal**—Specifies that the internal clock source is used. This is the default for T3.
		• **line**—Specifies that the network clock source is used. This is the default for E3.

Step 7	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration mode and returns to privileged EXEC mode.

Configuring DSU Mode and Bandwidth for E3

Perform this task to specify the interoperability mode used by an E3 controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial** *slot*/*port*
4. **dsu mode** {**0** | **1**}
5. **dsu bandwidth** *kbps*
6. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 3	**interface serial** *slot***/***port* **Example:** `Router(config)# interface serial 1/1`	Enters interface configuration mode and specifies the serial interface created on the controller.

Step 4	**dsu mode** {**0** | **1**}
	
	Example:
	`Router(config-if)# dsu mode 0`
		Specifies the interoperability mode used by an E3 controller.
		• **0**—Sets the interoperability mode to 0. This is the default. Specify mode 0 to connect an E3 controller to another E3 controller or to a Digital Link DSU (DL3100). Bandwidth range is from 358 to 24500/34010 kbps.
		Note If the bandwidth is set to greater than 24500 kbps, it defaults to 34010 kbps.
		• **1**—Sets the interoperability mode to 1. Specify mode 1 to connect an E3 controller to a Kentrox DSU. Bandwidth range is from 500 to 34010 kbps.

Step 5	**dsu bandwidth** *kbps* **Example:** `Router(config-if)# dsu bandwidth 44210`	Specifies the maximum allowable bandwidth in the range from 22 to 34010 kbps. • The real (actual) vendor-supported bandwidth is in the range from 358 to 34010 kbps. **Note** For the Cisco 2650XM and Cisco 2651XM platforms only, we recommend that you set the DSU bandwidth to 15000 in any subrate mode.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Scrambling for E3

Perform this task to enable encryption of the payload on the E3 controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial** *slot*/*port*
4. **scramble**
5. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface serial** *slot*/*port* **Example:** `Router(config)# interface serial 1/1`	Enters interface configuration mode.
Step 4	**scramble** **Example:** `Router(config-if)# scramble`	Enables the scrambling of the payload. • Default is off.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the BERT for E3

Perform this task to configure a BER test pattern on an E3 controller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller t3** *slot*/*port*
4. **bert pattern** {**2^23** | **2^20** | **2^15** | **1s** | **0s** | **alt-0-1**}
5. **no bert**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`controller e3`** *`slot`***`/`***`port`*
	Example:
	`Router(config)# controller e3 1/0`
		Selects the E3 controller and enters controller configuration mode.
		• *slot***/***port*—Backplane slot number and port number on the controller.

Step 4	**`bert pattern`** {**`2^23`** | **`2^20`** | **`2^15`** | **`1s`** | **`0s`** | **`alt-0-1`**}
	Example:
	`Router(config-controller)# bert pattern 2^20`
		Configures a bit error rate test pattern.
		• Acceptable values are:
		– **2^23**—Pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
		– **2^20**—Pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
		– **2^15**—Pseudorandom 0.151 test pattern that is 32,768 bits in length.
		– **1s**—Repeating pattern of ones (...111...).
		– **0s**—Repeating pattern of zeros (...000...).
		– **alt-0-1**—Repeating pattern of alternating zeros and ones (...01010...).

Step 5	**`no bert`**
	Example:
	`Router(config-controller)# no bert`
		Disables the BERT test pattern.

Step 6	**`exit`**
	Example:
	`Router(config-controller)# exit`
		Exits controller configuration mode and returns to privileged EXEC mode.

Configuring Loopback for E3

Perform this task to loop an entire E3 line toward the line and back toward the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller e3** *slot*/*port*
4. **loopback** {**local** | **network** {**line** | **payload**}}
5. **no loopback**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`controller e3`** *`slot`*/*`port`*
	Example:
	`Router(config)# controller e3 1/1`
		Selects the E3 controller and enters controller configuration mode.
		• *slot*/*port*—Backplane slot number and port number on the controller.

Step 4	**`loopback`** {**`local`** | **`network`** {**`line`** | **`payload`**}}
	Example:
	`Router(config-controller)# loopback local`
		Loops the E3 line toward the line and back toward the router,
		• **local**—Loops the data back toward the router and sends an AIS signal out toward the network.
		• **network** {**line** | **payload**}—Sets the loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**).

Step 5	`no loopback`
	Example:
	`Router(config-controller)# no loopback`
		Removes the loop.

Step 6	`exit`
	Example:
	`Router(config-controller)# exit`
		Exits controller configuration mode and returns to privileged EXEC mode.

Configuring National Bit for E3

Perform this task to set the E3 national bit in the G.751 frame used by the E3 controller. This configuration is used to set the bit when the E3 line crosses national boundaries.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller e3** *slot*/*port*
4. **national bit** {**1** | **0**}
5. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`controller e3 slot/port`
	Example:
	`Router(config)# controller e3 1/1`
		Selects the E3 controller and enters controller configuration mode.
		• *slot/port*—Backplane slot number and port number on the controller.

Step 4	`national bit {1	0}` **Example:** `Router(config-controller)# national bit 1`	Sets the E3 national bit in the G.751 frame used by the E3 controller. • **1**	**0**—Specifies the E3 national bit in the G.751 frame. • The default is 1.

Step 5	`exit`
	Example:
	`Router(config-controller)# exit`
		Exits controller configuration mode and returns to privileged EXEC mode.

Verifying the T3 or E3 Configuration

Perform this task to verify that the T3 or E3 controller is configured correctly. Enter the **show running-config**, **show controllers**, or **show interfaces serial** privileged EXEC command to display the command settings for the router.

Troubleshooting Tips

You can use the methods described in this section to troubleshoot the T3/E3 network module using Cisco IOS software.

Set Loopbacks

The T3/E3 local loopback can be used to ensure that the router and the T3/E3 network module are working properly. The controller clock source should be configured to “internal.”

Use T3/E3 network loopback and remote loopback to diagnose problems with cables between the T3/E3 controller and the central switching office at the link level. For this diagnostic setup to work, if the network module is looped toward the network, the network module must be configured with the clock source as “line.”

Run Bit Error Rate Test

The network module contains onboard BERT circuitry. With this circuitry present, the software can send and detect a programmable pattern that is compliant with CCITT/ITU pseudorandom and repetitive test patterns. BERT allows you to test cables and signal problems in the field.

When a BERT is running, your system expects to receive the same pattern that it is sending. To help ensure this, two common options are available.

- Use a loopback somewhere in the link or network.
- Configure remote testing equipment to send the same BERT pattern at the same time.

Please refer to the **bert pattern (t3/e3)** command in the “Command Reference” section for instructions on how to run BERT and check the results.

Use the show version Command

Use the **show version** command to learn if the router recognized the T3/E3 card and was able to initialize the card properly. The **show version** command lists the hardware interfaces and controllers present in the router. You should find “1 Subrate T3/E3 port(s)” as shown in the following example.

```
Router# show version
.
.
.
Router uptime is 2 hours, 6 minutes
System returned to ROM by power-on
System image file is “flash:c3725-i-mz”

cisco 3725 (R7000) processor (revision 0.4) with 111616K/19456K bytes of memory.
Processor board ID 12345678901
R7000 CPU at 240Mhz, Implementation 39, Rev 3.3, 256KB L2 Cache
Bridging software.
X.25 software, Version 3.0.0
Primary Rate ISDN software, Version 1.1
2 FastEthernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
2 Channelized T1/PRI port(s)
1 Subrate T3/E3 port(s)
DRAM configuration is 64 bits wide with parity disabled.
55K bytes of non-volatile configuration memory.
15680K bytes of ATA System CompactFlas (Read/Write)

Configuration register is 0x0
```

Configuration Example for the Clear Channel T3/E3 with Integrated CSU/DSU Feature

The following is sample output from the **show running-config** command for an E3 controller:

```
Router# show running-config

Building configuration...
%AIM slot 0 doesn't exist

Current configuration :1509 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
card type e3 1
no logging console
!
ip subnet-zero
no ip routing
!
!
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
!
controller E3 1/0
 clock source internal
!
!
!
!
interface Loopback0
 no ip address
 no ip route-cache
 shutdown
 no keepalive
!
interface FastEthernet0/0
 ip address 10.0.145.34 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 no cdp enable
!
```

```
interface Serial0/0
 no ip address
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 shutdown
 clockrate 2000000
 no fair-queue
!
interface FastEthernet0/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no keepalive
 no cdp enable
!
interface Serial0/1
 no ip address
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 shutdown
 clockrate 2000000
!
interface Serial0/2:0
 ip address 172.27.27.2 255.255.255.0
 no ip route-cache
 no keepalive
!
interface Serial1/0
 no ip address
 no ip route-cache
 no keepalive
 dsu bandwidth 34010
!
ip classless
no ip http server
!
ip pim bidir-enable
!
!
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
```

```
!
end
```

Additional References

The following sections provide additional references related to the Clear Channel T3/E3 with Integrated CSU/DSU feature:

- Related Documents, page 360
- Standards, page 360
- MIBs, page 360
- RFCs, page 361

Related Documents

Related Topic	Document Title
Basic information about configurations	*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
Detailed information about configuring interfaces	*Cisco IOS Interface Configuration Guide*, Release 12.2
Detailed information about Cisco IOS commands	*Cisco IOS Interface Command Reference*, Release 12.2 T
Detailed information about configuring voice, video, and fax applications	*Cisco IOS Voice, Video, and Fax Configuration Guide,* Release 12.2
Detailed information about Cisco IOS commands	*Cisco IOS Voice, Video, and Fax Command Reference,* Release 12.2 T
Information on connecting network modules	*Connecting T3/E3 Network Modules,* Release 12.2

Standards

Standards	Title
None	

MIBs

MIBs	MIBs Link
• RFC 1407 MIB • CISCO-ICSUDSU-MIB	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

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

RFCs	Title
RFC 1407	*Definitions of Managed Objects for the DS3/E3 Interface Type*

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, tools, and lots more. 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 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.

- **bert pattern (t3/e3)**
- **cablelength (t3)**
- **card type (t3/e3)**
- **clock source (t3/e3)**
- **controller e3**
- **dsu bandwidth (e3)**
- **dsu bandwidth (t3)**
- **dsu mode (e3)**
- **dsu mode (t3)**
- **framing (e3)**

- **framing (t3)**
- **loopback (e3)**
- **loopback (t3)**
- **mdl (t3)**
- **national bit (e3)**
- **scramble (t3/e3)**
- **show controllers (t3/e3)**

Glossary

backplane—The physical connection between an interface processor or card and the data buses and the power distribution buses inside a chassis.

BER—bit error rate. Ratio of received bits that contain errors.

CSU—channel service unit. Digital interface device that connects end-user equipment to the local digital telephone loop. Often referred to together with DSU as CSU/DSU.

DS-3—digital signal level 3. Framing specification used for sending digital signals at 44.736 Mbps on a T3 facility.

DSU—data service unit. Device used in digital transmission that adapts the physical interface on a DTE device to a transmission facility, such as T1 or E1. The DSU also is responsible for such functions as signal timing. Often referred to together with CSU as CSU/DSU.

E3—Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. E3 lines can be leased for private use from common carriers.

FEAC—far-end alarm code.

Frame Relay— industry-standard, switched data link layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it generally is considered a replacement.

HDLC—High-Level Data Link Control. Bit-oriented synchronous data link layer protocol developed by ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

MDL—Maintenance Data Link (MDL) message defined in the ANSI T1.107a-1990 specification. Also, the Cisco Message Definition Language—a high-level language used to specify protocols and protocol conversion operations on the VSC.

OIR—online insertion and removal. Feature that permits the addition, the replacement, or the removal of cards without interrupting the system power, entering console commands, or causing other software or interfaces to shut down.

PPP—Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

Subrate—Less than the standard rate of transmission, which is defined at the voice-grade rate of 64 kbps.

T3—Digital WAN carrier facility. T3 sends DS3-formatted data at 44.736 Mbps through the telephone switching network.

TDM—time-division multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single wire based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to send.

NM-AIC-64, Contact Closure Network Module

Feature History

Release	Modification
12.2(2)XG	This feature was introduced on the Cisco 2600 series and Cisco 3600 series platforms.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T and support for the Cisco 3631 was added.

This feature module describes the software support for the Network Module-Alarm Interface Controller-64 (NM-AIC-64), Contact Closure Network Module, commonly called the alarm interface controller (AIC). It includes information on the benefits of the new feature, supported platforms, and related documents.

This document includes the following sections:

Feature Overview

The NM-AIC-64, Contact Closure Network Module (also known as the AIC) is an optional card that expands network management capabilities for customer-defined alarms. The AIC has its own CPU that communicates with the router and external media through serial communication channels. The AIC reduces service provider and enterprise operating costs by providing a flexible, low-cost network solution for migrating existing data communications networks (DCNs) to IP-based DCNs. The AIC provides its users with a single box solution because it can be configured in the same router along with other operations, alarm administration, maintenance management, and provisioning (OAM&P) interfaces.

More than one AIC can be installed per router. For example, a Cisco 3662 can support up to six AICs. The Cisco 3640 can have up to three AICs, with the fourth slot reserved for communication, and so forth.

The AIC provides a total of 64 alarm inputs. Eight of the 64 points are software configurable for measuring either analog inputs or discrete inputs. The remaining 56 points are fixed to measure discrete points only. The AIC also provides 16 control relay outputs.

The discrete alarm input can be activated through ground or negative battery input. The negative battery range is -36 to -72V. The analog alarm is software configurable for either DC voltage or current. It can measure voltage from -60 to 60V or current from 0 to 20mA, but the configurable range is 4 to 20mA. The standard 16 control relays can be configured to turn on or turn off an external device.

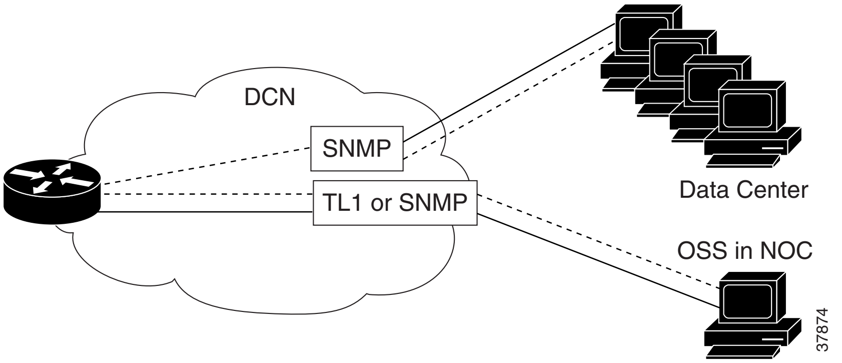
The AIC's 64 input contact points can control and monitor network elements and other nonintelligent interfaces, permitting the detection and report of alarms such as the following:

- Network element alarm states
- Building security (door and window open and close)
- Fire and smoke indication
- Building environmentals (temperature and humidity)
- Utility power readings

When an event occurs, such as a door alarm or an open gate, the AIC maps the simple discrete and analog alarms to preprogrammed intelligent messages and transports the messages to destinations in the IP network, typically to a network operations center (NOC). These messages are generated either in Transaction Language 1 (TL1) or in Simple Network Management Protocol (SNMP), which are used by a NOC's operations support system (OSS).

When the AIC is incorporated into the Cisco's DCN solution platforms, all the AIC's contact-closure alarms are routed and reported through the same network and systems as the intelligent network elements (NEs). This facilitates continued use of the existing OSS and its associated networks. A Cisco router with a AIC sends TL1 or SNMP messages to the OSS autonomously or in response to TL1 or SNMP commands from the OSS, as shown in Figure 40. TL1 supports two sessions, with the port numbers 5011 and 5012, respectively and SNMP supports four sessions.

Figure 40 TL1 and SNMP Message Flow in a DCN Application

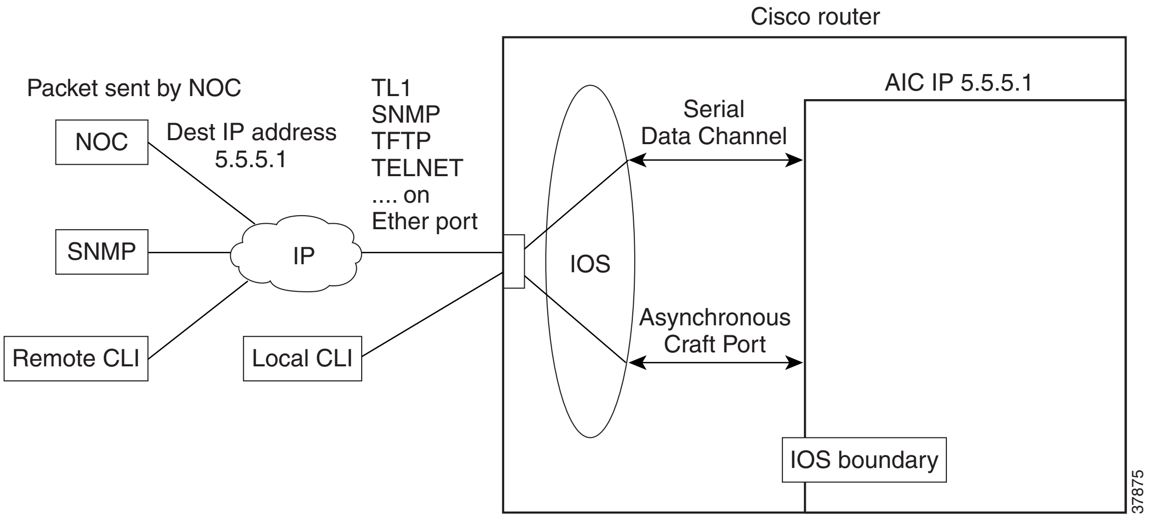


Serial Communications Channels

As illustrated in Figure 41, the AIC has two serial communications channels that provide different types of interfaces to the Cisco IOS:

- Serial data channel
- Asynchronous craft port

Figure 41 OS Boundary into the AIC



Serial Data Channel

The serial data channel supports all TCP/IP traffic to and from the AIC. This includes communication over IP with NOCs and data centers. The channel consists of one physical interface that provides support for the following applications:

- Telnet
- TL1
- TFTP
- SNMP

The Cisco IOS assigns an IP address to the AIC for use by the serial data channel. To route traffic, the serial data channel uses IP over synchronous high-level data link control (HDLC). All IP packets coming to the Cisco router with a destination IP address that matches the AIC's IP address are forwarded to the serial data channel using IP over HDLC.

Asynchronous Craft Port

The asynchronous craft port supports Telnet to the AIC's port number. This Telnet method, called local-CLI, is useful for debugging when remote Telnet to the AIC's IP address (remote-CLI) is not applicable. For more information, see the Configuring the NOC IP Address section.

The asynchronous craft port also supports an AIC boot sequence, similar to the ROM monitor in Cisco IOS, which allows you to recover from a corrupted software image or configuration. See the Override section.

Configuring the AIC

From a top-level view, AIC configuration involves assigning an IP address to the AIC using Cisco IOS commands and setting up alarm configurations with either TL1 or the AIC command-line interface (CLI). The flexible TL1 and AIC CLI permit a broad range of alarm configuration scenarios. The following are examples of four possible alarm configurations that can be programmed with the AIC CLI.

Configuring a Discrete Alarm

```
enable
config terminal
alarm 1
description "west door"
normally closed
description normal "door closed"
description alarm "door open"
level 2
exit
```

Configuring an Analog Alarm as an Analog Monitoring Voltage

```
enable
config terminal
alarm 57
analog voltage 2.5 30 60 60
description "tank level"
description normal "full"
description low "low"
description low-low "empty"
exit
```

Configuring an Analog Alarm as a Discrete Monitoring Current

```
enable
config terminal
alarm 58
description "east door"
discrete current-loop 0.0 3.2 5.9 high
exit
```

Configuring an Analog Alarm as a Discrete Monitoring Voltage

```
enable
config terminal
alarm 58
description "backup battery"
discrete voltage 9.0 high
exit
```

Configuring an Analog Alarm to Act Like a Discrete Alarm (Minimal Configuration Method)

```
enable
config terminal
alarm 59
discrete
exit
```

Benefits

Increased Functionality and Versatility

The AIC increases the functionality and versatility of the Cisco 2600 series, Cisco 3640, Cisco 3660, and Cisco 3662, giving service providers and enterprises enhanced communications and connections between the OSS and the NOC.

Low Cost Migration to Cost-Effective Technology

The AIC provides a flexible, low-cost network solution for service providers and enterprises to migrate existing DCNs to IP-based DCNs and to bridge traditional operations networks to a more cost-efficient, next generation, IP-based operations network.

Efficient, Single-Box Solution

The AIC provides discrete and analog alarms and initiated surveillance messages for central office and branch office network equipment (with nonintelligent interfaces) within the Cisco DCN solution products. By providing the contact closure network module in the same box as all the other OAM&P intelligent interfaces, customers benefit from the cost savings of a single-box solution that facilitates further DCN consolidation.

Streamlines Management and Implementation

The AIC's single-box solution simplifies service providers' network management processes. It also streamlines the installation of a solution for contact closure alarms because it reduces the number of external elements required to carry out such a function. This is especially beneficial to competitive local exchange carriers (CLECs) entering into a central office co-location situation where space is at a premium.

Restrictions

- The **no cdp enable** command is the only one that can be used on the AIC serial data channel. No other Layer 2 parameters on the AIC's serial data channel can be changed.
- Asynchronous communication parameters of the asynchronous craft port cannot be changed.

Related Documents

Cisco Documents

- *Update to the Cisco Network Module Hardware Installation Guide*
- *Release Notes for Network Module-Alarm Interface Controller-64 System Firmware on Cisco 2600 and Cisco 3600 Series Routers*

Other Documents

- Information about TL1 commands can be found in the Telcordia Technology (formerly Bellcore) document *Network Maintenance: Network Element and Transport Surveillance Messages*, GR-833-CORE, Issue 5, November 1996.
- For a reference of security-related commands (ACT-USER and CANC-USER), refer to Telcordia Technology's *Operations Applications Messages-Network Element and Network System Security Admin Messages*, TR-NWT-000835, Issue 2, January 1993.

Supported Platforms

- Cisco 2600 series
- Cisco 3600 series (Cisco 3631, 3640, and 3660)

Determining 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 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 verifies that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password are 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

No new or modified standards are supported by this feature.

MIBs

The AIC introduces a new MIB called CISCO-AIC-MIB. To support the AIC, an AIC object type and AIC ID were added to the following MIBs:

- OLD-CISCO-CHASSIS-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB

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

See the following sections for configuration tasks for the AIC feature:

- Configuring the AIC (required)
  - Entering Alarm Configuration Mode and Configuring the AIC IP Address
  - Configuring the IP Route to the AIC
- Configuring the NOC IP Address (optional)
- Configuring Alarms (optional)

Configuring the AIC

Cisco IOS commands are used for configuring the AIC IP address and the IP routing to the AIC. After the IP address and the IP routing are set, alarm configurations can then be set up with either TL1 or the AIC command-line interface. See Configuring the NOC IP Address or Configuring Alarms sections for more information.

The following sections describe how to configure the AIC IP address and the IP routing to the AIC.

Entering Alarm Configuration Mode and Configuring the AIC IP Address

Enter alarm configuration mode and configure the AIC IP address, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# show run`	Determines if the AIC is installed correctly in the router. If the AIC has been installed correctly, then the following appears: `interface serial slot/port` where the slot is the slot in which the AIC is inserted, and the port is 0.
Step 2	`Router# configure terminal`	Starts the configuration session.
Step 3	`Router(config)# alarm-interface slot-number`	Enters the AIC interface mode, specifying the slot number into which the AIC is installed.
Step 4	`Router(config-aic)# ip address ip-address`	Enters the IP address of the AIC.

	Command	Purpose
Step 5	`Router(config-aic)# reset`	Resets the AIC. Changing the IP configuration may not take until the next time the card is started. The **reset** command restarts the card.
Step 6	`Router(config-aic)# exit`	Exits the AIC interface mode.

Configuring the IP Route to the AIC

There are many ways to configure IP routing to the AIC. The first method, shown below, uses an unnumbered IP address. An administrator uses this method to assign an IP address that is already known to the router, such as an address that is one of the addresses in the subnet of a Fast Ethernet IP address.

Configure IP routing to the AIC, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **ip route** *network-number network-mask* {*IP address* | *interface*} [*distance*] [**name** *name*]	Establishes the discrete IP route and mask on the router's serial interface. The arguments have the following meanings: *network-number*—IP address of the target network or subnet. *network-mask*—Network mask that lets you mask network and subnetwork bits. *IP address*—Internet address of the next hop that can be used to reach that network in standard IP address notation. Example: 10.1.1.1. *interface*—Network interface to use. *distance*—(Optional) An administrative distance, which is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. **name** *name*—(Optional) Name of the user profile. Example: Router(config)# **ip route 5.5.5.1 255.255.255.255 serial2/0**
Step 2	Router(config)# **interface serial** *slot/port*	Enters the serial interface mode. Enter the slot in which the AIC is installed and the port 0.

	Command	Purpose
Step 3	Router(config-if)# **ip unnumbered** *type interface-number*	Enables IP processing on the serial interface to the AIC without assigning an explicit IP address to the interface. The *type* and *interface-number* arguments indicate another interface on which the router has an assigned IP address. The other interface cannot be an unnumbered interface, because only an interface that has its own IP address can be used to lend its IP to the serial port. Enter, for example: Router(config-if)# **ip unnumbered FastEthernet 0/0**
Step 4	Router(config-if)# **exit**	Exits the serial interface mode.

The second method, shown below, does not use an unnumbered IP address and is used when there is a subnet available to the serial interface and to the AIC. Usually, this subnet is small with a subnet mask such as 255.255.255.252.

s

	Command	Purpose
Step 1	Router(config)# **interface serial** *slot/port*	Enters the serial interface mode. Enter the slot in which the AIC is installed and the port 0.
Step 2	Router(config-if)# **ip address** *ip-address network-mask*	Specifies the IP address and mask of the router's serial interface to the AIC. For example: Router(config)# **ip address 5.5.5.2 255.255.255.252**
Step 3	Router(config-if)# **exit**	Exits the serial interface mode.

Accessing the AIC

Remote-CLI and local-CLI are the two methods for accessing the AIC:

- Remote-CLI involves Telneting to the IP address of the AIC. For example:

  ```
  telnet 5.5.5.1
  ```

- Local-CLI involves accessing the asynchronous craft port by Telneting to the IP address of the router and the AIC's TCP port number. For example:

  ```
  telnet 10.2.130.105 2001
  ```

  where 10.2.130.105 is the router's IP address and 2001 is on slot 0 of the router.

  The AIC's TCP port number depends on the slot number in which the AIC is installed. As shown in Table 26, Part 1, the Cisco IOS software reserves the first line of each slot for the asynchronous craft port.

Table 26, Part 1 TCP Port Number Allocation for the AIC on the Cisco 2600 and Cisco 3600 Series

Slot Number	Terminal Line Number for the AIC's Asynchronous Craft Port	TCP Port Number
0	1	2001
1	33	2033
2	65	2065
3	97	2097
4	129	2129
5	161	2161
6	193	2193

Configuring the NOC IP Address

Configure up to four NOC IP addresses to which the AIC sends SNMP messages, beginning in global configuration mode.

Note For a complete listing of AIC CLI commands, see the AIC CLI Commands section.

	Command	Purpose
Step 1	`aic(config)# snmp`	Enters the SNMP configuration mode.
Step 2	`aic(config-snmp)# noc ip-address {number} ip-address`	Enters an NOC IP address in which the AIC sends SNMP messages. The *number* argument can be the numbers 1 through 4.
Step 3	`aic(config-snmp)# exit`	Exits the SNMP configuration mode.

Configuring Alarms

After the AIC and NOC IP addresses have been configured, you can configure alarms by programming the AIC's discrete and analog contact points. These tasks can be performed on-site or by Telneting as described in the Accessing the AIC section.

Alarms are configured using either TL1 or AIC CLI. Information about TL1 commands can be found in the Telcordia Technology (formerly Bellcore) document *Network Maintenance: Network Element and Transport Surveillance Messages*, GR-833-CORE, Issue 5, November 1996. For a reference of security-related commands (ACT-USER and CANC-USER), refer to Telcordia Technology's *Operations Applications Messages-Network Element and Network System Security Admin Messages*, TR-NWT-000835, Issue 2, January 1993. The following TL1 messages and commands are supported by the AIC:

- TL1 Messages
  - REPT-ALM-ENV
  - REPT-ALM-EQPT
  - REPT-EVT
- TL1 Commands

- ACT-USER
- CANC-USER
- OPR-EXT-CONT
- RTRV-EXT-CONT
- RLS-EXT-CONT
- RTRV-ALM
- RTRV-ALM-ENV
- RTRV-ATTR
- RTRV-ATTR-CONT
- RTRV-ATTR-ENV
- RTRV-ATTR-LOG
- RTRV-HDR
- RTRV-LOG
- SET-ATTR-EQPT
- SET-ATTR-LOG
- SET-ATTR-ENV
- STA-LOG
- STP-LOG

Programming the Analog Contact Points

Alarm points 57 through 64 are analog inputs, which are configurable as discrete inputs. When configured as an analog input, you must select whether the point is monitoring voltage or current. You must also define five ranges by selecting four values for a point-monitoring voltage or six ranges for a point-monitoring current. For current-monitoring points, the lowest and highest values define the range of possible values. (Valid values are from –99999.9 to 99999.9.) For voltage-monitoring alarms, the range of possible values is always –60 to 60V. The other four values must be within the defined range, and they partition the range into low-low, low, high, and high-high ranges. Except for the normal range, each range is associated with an alarm condition.

Analog points have four unique alarm states. Each alarm state has its own alarm description string. Only one alarm state per point may be active at any given time. In other words, when a threshold is crossed, the previous alarm state is cleared and the new alarm state is active.

When an analog input is configured as discrete, you must select whether the point is monitoring voltage or current. Similar to the analog configuration, you must also select the range of acceptable values for a current-monitoring alarm. (Valid values are from –99999.9 to 99999.9.) The voltage range is always –60 to 60V. You must define the threshold that causes the alarm condition and whether the normal state of the alarm is the higher or lower range.

Note For the current analog point, the lower boundary is 4 mA and the upper boundary is 20 mA. For example,

```
analog current-loop 10 13 16 17 20 26
```

has 16 units between 10 and 26. If the AIC measures 4 mA, then it factors that the point is registering at the lower boundary. The AIC interprets 13 as 7 mA, 16 as 10 mA, 17 as 11 mA, 20 as 14 mA, and 26 as the upper boundary, which is 20 mA.

Following are examples:

Point 57 is monitoring ambient temperature of a building and the sensor range is –20 to 75 degrees Celsius. Below 0 degrees is a critical alarm, 0 to 10 degrees is a major alarm, 10 to 35 degrees is the normal range, 35 to 45 degrees is a minor alarm, and above 45 degrees is a major alarm. The configuration for this point follows:

```
alarm 57
analog current-loop -20 0 10 35 45 75
level low-low 1
level low 2
level high 3
level high-high 2
```

Point 58 is monitoring a fuel tank level with a resistive sensor. Below –46 volts is a critical alarm, –46 to –40 volts is a minor alarm, and above –40 volts is the normal range. This is a unidirectional alarm, so the high thresholds are set equal to the high bound (since this threshold cannot be crossed). The configuration for this point follows:

```
alarm 58
analog voltage -46 -40 60 60
level low-low 1
level low 3
```

Point 59 is monitoring a battery bank. Below –42 volts is a critical alarm and above –42 volts is the normal range. The configuration for this point follows:

```
alarm 59
discrete voltage -42 high
level 1
```

Programming the Discrete Contact Points

The discrete alarms do not require as much programming as the analog alarms. The AIC CLI commands available are the following:

no	Reversal option
exit	Exits current mode
description	See Alarm Subconfiguration Mode See Control Subconfiguration Mode
normally	See Alarm Subconfiguration Mode
level	See Alarm Subconfiguration Mode

Verifying the IP Address

To verify that the correct AIC IP address and IP route were entered, use the **show run** command. Below are samples of before-configuration and after-configuration **show run** outputs:

```
interface Serial5/0
 ip unnumbered FastEthernet0/0
```

```
!
ip route 10.2.130.102 255.255.255.255 Serial5/0
!
alarm-interface 5
 ip address 10.2.130.102
```

********before configuration **show run** output*******

```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uut2-3660
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
!
call rsvp-sync
cns event-service server
!
!
interface FastEthernet0/0
 ip address 10.2.130.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface Serial5/0
 no ip address
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip http server
!
no cdp run
!
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
 transport input none
line 161
 no exec
 transport preferred none
 transport input telnet
 transport output none
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
end
```

*****after configuration **show run** output*******

```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uut2-3660
!
logging rate-limit console 10 except errors
no logging console
!
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
!
call rsvp-sync
cns event-service server
!
interface FastEthernet0/0
 ip address 10.2.130.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface Serial5/0
ip unnumbered FastEthernet0/0
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip route 10.2.130.102 255.255.255.255 Serial5/0
ip http server
!
no cdp run
!
!
alarm-interface 5
 ip address 10.2.130.102
!
dial-peer cor custom
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line 161
 no exec
 transport preferred none
 transport input telnet
 transport output none
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
```

```
end
```

Troubleshooting Tips

If no alarm messages are sent for an unusually long period of time, **ping** the AIC address to check for connectivity.

For more information about error messages, refer to the *Release Notes for Network Module-Alarm Interface Controller-64 System Firmware on Cisco 2600 and Cisco 3600 Series Routers*.

Monitoring and Maintaining the AIC

The AIC provides a TFTP client for software upgrade and configuration image transfer. The methods for both actions, as well as how to override the existing software or configuration, are described below.

Software Upgrade

When upgrading software, you must reset the AIC to run the new software. The AIC provides a protected (login required) command for software download. When you invoke this command with the TFTP server address as a parameter, the AIC connects to the IP address and, via TFTP, retrieves the software image file. After verifying that the software has been transferred successfully, the AIC replaces its running software with the newly downloaded software.

In the case of incompatible versions of IOS and AIC software, the IOS recognizes the difference and displays this information to you. You make the decision whether to upgrade or downgrade either the IOS or AIC software or to take no corrective action.

Configuration Backup

The AIC CLI provides commands for storing and restoring configurations. Users can transfer the current configuration of the AIC to or from the TFTP server whose address is given as a parameter to the **put** or **get config** command. When a configuration file is transferred from the server to the AIC, the AIC takes on the new configuration.

The configuration is stored as a list of commands (script) that can be applied to the CLI of a AIC for configuration.

Two other useful commands are **get image** and **put config**. Use **get image** to get a new image, and **put config** to back up the configuration to the TFTP server.

Backup is not automatic, but the AIC reminds you, upon logout, to back up the configuration.

Override

In the case that bad software is resident on the AIC or that the configured administrator password is lost, the AIC provides a method for recovering the card. Upon booting, the AIC begins a countdown, visible at the AIC local CLI (craft port). If an ASCII character is received on that local CLI channel (DSCC4 channel 2) during this countdown, the AIC enters a mode in which a limited CLI is available. At this limited CLI, available over the craft port only, no login is necessary. You may execute commands for software upgrade or restore the configuration to its default. The restored default configuration takes effect upon a reset of the AIC card. See **reset (alarm-interface)** for more information.

After interrupting the countdown, you see an "[AIC Boot]:" prompt. From this prompt, you can enter "?" to see the available commands, "g" to **get** a new application image, or "d" to **delete** the current configuration and return to the defaults. (All commands require a carriage return.) In the case of the **get** command, you are prompted for the name of the file, the IP address of the TFTP server, and a confirmation.

Show Commands

The Cisco IOS **show** commands can be used to display AIC configuration settings and the information sent to the IOS by the AIC. The **ping** command is useful for verifying asynchronous line connectivity.

The following Cisco IOS **show** command can be used to monitor and maintain alarms:

Command	Purpose
`Router#` **`show alarm-interface`** `[`*`slot-number`*`] [summary]`	Displays AIC configuration setting and the information sent to the IOS by the AIC.

A list of the AIC CLI **show** commands can be found in the User Mode section.

Configuration Examples

This section provides the following configuration examples:

- Configuring the AIC IP Address
- Configuring IP Route to the AIC
  - With an Unnumbered IP Address
  - Without an Unnumbered IP Address
- AIC CLI Configuration for Alarms

Configuring the AIC IP Address

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
!
hostname router
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
interface FastEthernet0/0
ip address 10.2.130.5 255.255.0.0
duplex auto
speed auto
no cdp enable
```

```
!
interface Serial1/0
ip address 172.128.12.1 255.255.255.252
!
ip kerberos source-interface any
ip classless
no ip http server
!
!
alarm-interface 1
ip address 172.128.12.2
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
transport input none
line 33
no exec
transport preferred none
transport input telnet
transport output none
stopbits 1
line aux 0
line vty 0 4
password lab
login
!
no scheduler allocate
!
end
```

Configuring IP Route to the AIC

With an Unnumbered IP Address

```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uut2-3660
!
logging rate-limit console 10 except errors
no logging console
!
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
!
call rsvp-sync
cns event-service server
!
interface FastEthernet0/0
 ip address 10.2.130.2 255.255.0.0
 duplex auto
 speed auto
```

```
no cdp enable
!
interface Serial5/0
 ip unnumbered FastEthernet0/0
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip route 10.2.130.102 255.255.255.255 Serial5/0
ip http server
!
no cdp run
!
alarm-interface 5
 ip address 10.2.130.102
!
dial-peer cor custom
!
!
!
line con 0
 exec-timeout 0 0
 transport input none
line 161
 no exec
 transport preferred none
 transport input telnet
 transport output none
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
end
```

Without an Unnumbered IP Address

```
uut5-2621#s run
Building configuration...

Current configuration :1318 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uut5-2621
!
logging rate-limit console 10 except errors
no logging console
!
ip subnet-zero
!
no ip finger
no ip domain-lookup
!
no ip dhcp-client network-discovery
!
interface FastEthernet0/0
```

```
 ip address 10.2.130.5 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface Serial1/0
 ip address 172.128.12.1 255.255.255.252
!
router rip
 network 10.0.0.0
!
ip kerberos source-interface any
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.1
no ip http server
!
no cdp run
!
snmp-server packetsize 4096
snmp-server manager
!
!
alarm-interface 1
 ip address 172.128.12.2
call rsvp-sync
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
 transport input none
line 33
 no exec
 transport preferred none
 transport input telnet
 transport output none
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
no scheduler allocate
!
end
```

AIC CLI Configuration for Alarms

These examples are output from the command **show alarm config #** command.

Discrete Alarm

```
description:west door
normally closed
normal state description:door closed
alarm state description:door open
alarm Level: 4
SNMP trap:enabled
```

Analog Alarm Monitoring Current

```
description: thermostat
high-high state description: very hot
high-high Level: 4
high state description: hot
high Level: 4
normal state description: just right
low state description: cold
low Level: 4
low-low state description: very cold
low-low Level: 4
current-loop -5.2 5.4 15.0 25.0 35.1 45.6
SNMP trap: enabled
```

Analog Alarm Monitoring Current Configured as a Discrete

```
description:east door
configured as discrete
normal state description:door closed
alarm description:door open
alarm Level: 4
current-loop 0.0 3.2 5.9
normally high
SNMP trap:enabled
```

AIC CLI Syntax

The AIC CLI operates in four separate modes as described below. The mode currently in use determines the prompt used and the commands that are available. The modes are designed to mimic the modes available at the Cisco CLI:

.

User Mode

The interface begins in user mode. This mode is not password-protected, by default, although it may be configured to be. In user mode, commands that show information are available. Also available is the command for entering privileged mode. The prompt in user mode is the AIC name followed by a right angle bracket (>).

Privileged Mode

In privileged mode, configuration may be viewed and all user mode commands are available. Also available are the commands for reentering user mode and entering configuration modes. The prompt in privileged mode is the AIC name followed by a pound sign (#).

Upon entrance to privileged mode, if one or more users are already using privileged mode (or any configuration mode), the entering user is warned that those other users may be configuring the AIC.

Global Configuration Mode	Global configuration mode allows configuration of global options and allows you to enter the subconfiguration modes. The commands available here are not available in other modes. The prompt in this mode is the AIC name followed by (config)#.
Subconfiguration Modes	The subconfiguration modes are used for configuring specific parts of the AIC. Commands available in this mode are not available in other modes. Four subconfiguration modes are available: alarm, control, TL1, and SNMP. The prompts in these modes are the AIC name followed by (config-alarm)#, (config-control)#, (config-tl1)#, and (config-snmp)#.

AIC CLI User Levels

The AIC allows for three levels of users. For purposes of generality, in this document, the levels are referred to by number, where 1 is the most privileged level and 3 is the least privileged. Level 3 users are allowed to enter user mode only. Level 1 and 2 users are able to access all modes, but not all commands are available to level 2 users. The command descriptions indicate to which levels of users the command is available.

Login requirements are configurable. By default, login is required for privileged users (levels 1 and 2), but not for level 3 users. Login requirements can be configured so that login is required for users of all levels.

AIC CLI Error Handling

If an AIC CLI command is entered incorrectly, an error message is displayed one line below the input, with a caret (^) indicating the invalid parameter.

AIC CLI Commands

The command syntax and description for each command is shown below, organized by the mode in which the command is available.

The syntax of the commands includes the following symbols:

- #—number, validated according to requirements
- #.#.#.#—IP address
- $—string surrounded by double " ", validated according to requirements
- <>—optional part of command

User Mode

enable

Enters privileged mode. This command is available to level 1 and 2 users.

exit

Exits the AIC CLI. This command is available to level 1, 2, and 3 users.

show tl1 alarm

Displays TL1 attributes for every alarm point in the following format. This command is available to level 1, 2, and 3 users.

```
point 1
sid: router 3
aid: slot 2
cond: point 1
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend

point 2
sid: router 3
aid: slot 2
cond: point 2
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend

...
```

show tl1 alarm

Displays TL1 attributes for the specified alarm point in the following format. This command is available to level 1, 2, and 3 users. The output format for alarms 1 to 56 is followed by the output format for alarms 57 to 64.

```
sid: router 3
aid: slot 2
cond: point 16
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend

sid: router 3
aid: slot 2
cond: point 60
eqpt: eqpt
env: false
srveff: nsa
dirn: trmt
locn: nend
```

show tl1 control

Displays TL1 attributes for every control in the following format. This command is available to level 1, 2, and 3 users.

```
point 1
sid: router 3
```

```
aid: slot 2
cond: point 1
durn: 3.0 sec

point 2
sid: router 3
aid: slot 2
cond: point 2
durn: 3.0 sec

...
```

show tl1 control

Displays TL1 attributes for the specified control in the following format. This command is available to level 1, 2, and 3 users.

```
sid: router 3
aid: slot 2
cond: point 1
durn: 3.0 sec
```

show snmp config

Displays the GET and TRAP community names and the SNMP global option, alarm-off trap. This command is available to level 1, 2, and 3 users.

```
GET community name: public
TRAP community name: public
SNMP alarm-off trap: enabled
```

show snmp noc address list

Displays the four IP addresses to which SNMP traps are sent. This command is available to level 1, 2, and 3 users.

```
noc 1: 10.1.43.55
noc 2: 10.1.43.54
noc 3: 172.12.37.12
noc 4: 172.26.9.25
```

show snmp noc address

Displays the specified IP address to which SNMP traps are sent. This command is available to level 1, 2, and 3 users.

```
noc 3: 172.16.37.12
```

show ip-address

Displays the AIC’s IP address. This command is available to level 1, 2, and 3 users.

```
172.12.37.12
```

show clock

Displays the current date and time. This command is available to level 1, 2, and 3 users.

```
14:12:34 06/23/01
```

show history

Displays the last ten input commands, as shown below. If fewer than ten commands have been entered since reboot, only those are displayed. Commands are shown in order of input. The most recent command is at the bottom. This command is available to level 1, 2, and 3 users.

```
show clock
enable
configure terminal
alarm 1
description “west door”
description normal “door closed”
description alarm “door open”
normally closed
no normally closed
exit
```

show alarm state

Displays the states of every alarm. Points in the alarmed state are indicated by a number (1 to 4), indicating the level (1 is critical, 4 is status), as shown. This command is available to level 1, 2, and 3 users.

```
1......8 9.....16 17....24 25....32 33....40 41....48 49....56 57....64
-------- --13---- --4-44-- 3---2--- ---4432- -------- --1----- --444--4
```

show alarm state

Displays descriptions of the specified alarm point and the alarm state. This command is available to level 1, 2, and 3 users.

```
west door
normal
```

show alarm config

Displays the configuration of every alarm point. This command is available to level 1, 2, and 3 users.

```
point 1
description: alarm 1
normally open
normal state description: normal
alarm state description: alarm
alarm Level: 4
SNMP trap: enabled

point 2
description: alarm 2
normally closed
normal state description: normal
alarm state description: alarm
alarm Level: 4
SNMP trap: disabled

point 57
description: alarm 57
high-high state description: high-high
high-high Level: 4
high state description: high
high Level: 4
normal state description: normal
low state description: low
low Level: 4
low-low state description: low-low
low-low Level 4: low-low
current-loop 4.0 7.0 10.0 13.0 16.0 20.0
SNMP trap: enabled
```

show alarm config

Displays the configuration of the specified alarm. This command is available to level 1, 2, and 3 users. The output format for alarms 1 to 56 is followed by the output formats for alarms 57 to 64.

```
description: alarm 1
normally open
normal state description: normal
alarm state description: alarm
alarm Level: 4
SNMP trap: enabled

description: alarm 2
high-high state description: high-high
high-high Level: 4
high state description: high
high Level: 4
normal state description: normal
low state description: low
low Level: 4
low-low state description: low-low
low-low Level: 4
current-loop 4.0 7.0 10.0 13.0 16.0 20.0
SNMP trap: enabled
```

show control state

Displays information about the logical and physical states of all the control points. This command is available to level 1, 2, and 3 users.

```
1......8 9.....16
-------- -------- logical (-RELEASED, ^OPERATED)
-------- -------- physical (-OPEN, ^CLOSED)
```

show control state

Displays the logical and physical (in parentheses) states of the specified control point. This command is available to level 1, 2, and 3 users.

```
control 1
released latched (physically open)
```

show control config

Displays the configuration of every control point. This command is available to level 1, 2, and 3 users.

```
point 1
description: generator 1
enabled
normally open
momentary duration: 3.2 seconds

point 2
description: generator 2
enabled
```

```
normally open
momentary duration: 40.2 seconds
...
```

show control config

Displays the configuration of the specified control. This command is available to level 1, 2, and 3 users.

```
description: generator 2
enabled
normally open
momentary duration: 3.2 seconds
```

ping #.#.#.#

Sends a series of five ICMP echo request packets to the specified IP address and displays the results. Sample output is shown below. This command is available to level 1, 2, and 3 users.

```
aic# ping 10.2.0.1
Pinging IP address 1.2.0.1
Failure
Success
Success
Success
Success
Success rate is 80 percent (4/5)
aic#
```

Privileged Mode

All commands available in user mode are available in privileged mode.

exit

Reenters user mode. This command is available to level 1 and 2 users.

show users

Displays usernames and levels of access. Currently logged-in users are indicated by an asterisk (*). The user invoking this command is indicated by a right angle bracket (>). This command is available to level 1 and 2 users.

```
Level Username
>1     admin
 2     sue
*2     george
 2     noc1
 2     noc2
 2     noc3
 3     alvin
 3     simon
 3     ted
 3     unused4
 3     unused5
```

configure terminal

Enters global configuration mode. This command is available to level 1 and 2 users.

operate control # momentary

Operates the specified control momentarily, according to the configured length of operation. This command is available to level 1 and 2 users.

operate control # latch

Operates the specified control. This command is available to level 1 and 2 users.

release control # momentary

Releases the specified control momentarily according to the configured length of release. This command is available to level 1 and 2 users.

release control # latch

Releases the specified control. This command is available to level 1 and 2 users.

get image $ #.#.#.#

Retrieves the software image from the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

put image $ #.#.#.#

Transfers the running software image to the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

get config $ #.#.#.#

Retrieves the configuration file from the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

put config $ #.#.#.#

Transfers the configuration file to the specified IP address, according to the path and filename specified, via TFTP. This command is available to level 1 and 2 users.

Global Configuration Mode

exit

Reenters privileged mode. This command is available to level 1 and 2 users.

alarm

Enters alarm subconfiguration mode to configure the specified alarm number. This command is available to level 1 and 2 users.

control

Enters control subconfiguration mode to configure the specified control number. This command is available to level 1 and 2 users.

tl1

Enters TL1 subconfiguration mode. This command is available to level 1 and 2 users.

snmp

Enters SNMP subconfiguration mode. This command is available to level 1 and 2 users.

<no> name $

Configures the AIC's name to the specified string. If the <no> option is used, the name is set to the default value ("aic"). This command is available to level 1 and 2 users.

<no> user #1 #2 $1 $2

Assigns the first string as the username and the second string as the password for the specified user (second number) of the specified level (first number). If the <no> option is used, the string fields are not used and the username and password return to default values. The default string for both username and password for the level 1 user is "admin". The default strings for both username and password for level 2 users are "unused1", "unused2", and so on. The default strings for both username and password for level 3 users are "unused101", "unused102", and so on. This command is available to level 1 users.

<no> early-login

Requires login at entry to the AIC CLI (user mode) instead of at entry into privileged mode. If the <no> option is used, login is required at entry into privileged mode instead of at entry into user mode. This command is available to level 1 users.

Alarm Subconfiguration Mode

exit

Reenters global configuration mode. This command is available to level 1 and 2 users.

<no> description $

Sets the alarm's description to the specified string. If the <no> option is used, the string field is not required and the description is set to "alarm #", where # is the number of the alarm being configured. This command is available to level 1 and 2 users.

<no> description normal $

Sets the alarm's description of its normal state to the specified string. If the <no> option is used, the string field is not required and the description is set to "normal". This command is available to level 1 and 2 users.

<no> description alarm $

Sets the alarm's description of its alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to "alarm". While this string applies to points 57 to 64 only if configured as discrete, the command is always accepted. This command is available to level 1 and 2 users.

<no> description high-high $

Sets the alarm’s description of its high-high alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to “high-high”. While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

<no> description high $

Sets the alarm’s description of its high alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to “high”. While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

<no> description low $

Sets the alarm’s description of its low alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to “low”. While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

<no> description low-low $

Sets the alarm’s description of its low-low alarm state to the specified string. If the <no> option is used, the string field is not required and the description is set to “low-low”. While this string applies only to points 57 to 64 configured as analog alarms, the command is always accepted. This command is available to level 1 and 2 users.

<no> normally closed

Sets the alarm’s normal state to closed. If the <no> option is used, the normal state is set to open. This command applies only to points 1 to 56. This command is available to level 1 and 2 users.

<no> level

Sets the alarm’s level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies to points 57 to 64 only when configured as discrete, the command is always accepted. This command is available to level 1 and 2 users.

<no> level high-high

Sets the alarm’s high-high state level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

<no> level high

Sets the alarm’s high state level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

<no> level low

Sets the alarm's low state level to the specified level. If the <no> option is used, level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

<no> level low-low

Sets the alarm's low-low state level to the specified level. If the <no> option is used, the level field is not used and the level is set to the default level (4). While this level applies only to points 57 to 64 configured as analog, the command is always accepted. This command is available to level 1 and 2 users.

analog current-loop #1 #2 #3 #4 #5 #6

This command is only for alarm points 57 to 64. It configures the alarm points as a current-loop monitoring analog alarm, where #1 and #6 represent the low and high bounds of the range of current, respectively, and where #2, #3, #4, and #5 represent thresholds. These values may be no less than –9999999.9 and no more than 9999999.9. The values specified must be in increasing order. (#1 is less than or equal to #2, #2 is less than or equal to #3, and so on.) This command is available to level 1 and 2 users.

analog voltage #1 #2 #3 #4

This command is only for alarm points 57 to 64. It configures the alarm points as voltage monitoring analog alarms, where #1, #2, #3, and #4 represent thresholds. The values specified must be in increasing order. (#1 is less than or equal to #2, #2 is less than or equal to #3, and so on.) This command is available to level 1 and 2 users.

discrete current-loop #1 #2 #3 high

This command is only for alarm points 57 to 64. It configures the alarm points as discrete, where #1 and #3 represent the low and high bounds of the range, respectively; #2 represents the threshold that indicates the alarm; and the normal state is high. This command is available to level 1 and 2 users.

discrete current-loop #1 #2 #3 low

This command is only for alarm points 57 to 64. It configures the alarm points as discrete, where #1 and #3 represent the low and high bounds of the range, respectively; #2 represents the threshold that indicates the alarm; and the normal state is low. This command is available to level 1 and 2 users.

discrete voltage #1 high

This command is only for alarm points 57 to 64. It configures the alarm points as discrete alarm points, where #1 represents the threshold that indicates the alarm, and the normal state is high. The bounds of the range are always –60.0 and 60.0 volts. This command is available to level 1 and 2 users.

discrete voltage #1 low

This command is only for alarm points 57 to 64. It configures the alarm points as discrete alarm points, where #1 represents the threshold that indicates the alarm, and the normal state is low. The bounds of the range are always –60.0 and 60.0 volts. This command is available to level 1 and 2 users.

discrete

This command is only for alarm points 57 to 64. It configures the alarm points as discrete alarm points so that they resemble the discrete alarm points 1 to 56. This allows users a simple way to configure an analog alarm as discrete, so that it acts like other discrete points. To reverse the alarm or change the threshold, another command must be used. This command is available to level 1 and 2 users.

Control Subconfiguration Mode

exit

Reenters global configuration mode. This command is available to level 1 and 2 users.

<no> description $

Sets the control's description to the specified string. If the <no> option is used, the string field is not required and the description is set to "control #", where # is the number of the alarm being configured. This command is available to level 1 and 2 users.

<no> normally closed

Sets the control's normal state to closed. If the <no> option is used, the normal state is set to "open." This command is available to level 1 and 2 users.

<no> disable

Disables the control. If the <no> option is used, the control is enabled. This command is available to level 1 and 2 users.

<no> momentary timer

Sets the control's momentary duration to the specified number of seconds. Valid values range from 0.1 to 600.0, in increments of tenths. If the <no> option is used, the momentary duration is set to 3.0 seconds. This command is available to level 1 and 2 users.

TL1 Subconfiguration Mode

Note The TL1 parameters have limits on the number of characters that you can enter. To find the limits for a particular parameter, enter "?"

exit

Reenters global configuration mode. This command is available to level 1 and 2 users.

<no> alarm # sid $

Sets the TL1 source identifier (SID) of the specified alarm to the specified string. If the <no> option is used, the SID is set to "AIC". This command is available to level 1 and 2 users.

To find the limits for this parameter:

```
Router(config-tl1)# alarm 1 sid ?
```

```
                     WORD              SID string (20 character max)
```

<no> alarm # aid $

Sets the TL1 access identifier (AID) of the specified alarm to the specified string. If the <no> option is used, the AID is set to "UNDEFINED". This command is available to level 1 and 2 users.

<no> alarm # cond $

Sets the TL1 condition (COND) of the specified alarm to the specified string. If the <no> option is used, the COND is set to "POINT #", where # is the specified alarm number. This command only applies to points 57 to 64 when they are configured as discrete alarm points. This command is available to level 1 and 2 users.

<no> alarm # eqpt $

Sets the TL1 equipment (EQPT) of the specified alarm to the specified string. If the <no> option is used, the EQPT is set to "EQPT". This command is available to level 1 and 2 users.

<no> alarm # env

Sets the specified alarm as an environmental alarm (ENV = TRUE). If the <no> option is used, it is set as not an environmental alarm (ENV= FALSE). This command is available to level 1 and 2 users.

<no> alarm # srveff

Sets the specified alarm as service-affecting (SRVEFF = SA). If the <no> option is used, it is set as not service-affecting (SRVEFF = NSA). This command is available to level 1 and 2 users.

alarm # dirn trmt

Sets the TL1 direction (DIRN) of the specified alarm to transmit (TRMT). This command is available to level 1 and 2 users.

alarm # dirn rcv

Sets the TL1 direction (DIRN) of the specified alarm to receive (RCV). This command is available to level 1 and 2 users.

alarm # dirn na

Sets the TL1 direction (DIRN) of the specified alarm to NA. This command is available to level 1 and 2 users.

alarm # locn nend

Sets the TL1 location (LOCN) of the specified alarm to near-end (NEND). This command is available to level 1 and 2 users.

alarm # locn fend

Sets the TL1 location (LOCN) of the specified alarm to far-end (FEND). This command is available to level 1 and 2 users.

alarm # locn line

Sets the TL1 location (LOCN) of the specified alarm to line (LINE). This command is available to level 1 and 2 users.

<no> control # sid $

Sets the TL1 source identifier (SID) of the specified control to the specified string. If the <no> option is used, the SID is set to "AIC". This command is available to level 1 and 2 users.

<no> control # aid $

Sets the TL1 access identifier (AID) of the specified control to the specified string. If the <no> option is used, the AID is set to "UNDEFINED". This command is available to level 1 and 2 users.

<no> control # cond $

Sets the TL1 condition (COND) of the specified control to the specified string. If the <no> option is used, the COND is set to "POINT #", where *#* is the specified control number. This command is available to level 1 and 2 users.

SNMP Subconfiguration Mode

exit

Reenters global configuration mode. This command is available to level 1 and 2 users.

<no> community $

Sets the SNMP community name to the specified string. Community names for other operations are set to "public" and cannot be changed. If the <no> option is used, the community name is set to "aic snmp". This command is available to level 1 and 2 users.

<no> noc ip-address # #.#.#.#

Sets the specified number NOC address to the specified IP address. This also enables this NOC address. If the <no> option is used, the IP address is not used and the specified number NOC address is disabled. This command is available to level 1 and 2 users.

<no> disable alarm

Disables the sending of traps upon change of state of the specified alarm. If the <no> option is used, the traps are enabled for this alarm.

<no> disable alarm-off-trap

Disables the sending of traps upon change of state to the inactive state for all alarms. If the <no> option is used, the traps are enabled.

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.

New Commands

- **alarm-interface**
- **debug alarm-interface**
- **reset (alarm-interface)**
- **show alarm-interface**

Modified Commands

- **show diag**

Glossary

AIC—Alarm Interface Controller.

CiscoFusion—Cisco internetworking architecture that fuses together the scalability, stability, and security advantages of the latest routing technologies with the performance benefits of ATM and LAN switching, and the management benefits of VLANs. See also Cisco IOS.

Cisco IOS—Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms. See also CiscoFusion.

CLEC—Competitive local exchange carrier, CAP Competitive Access Provider. In the U.S., the Telecommunications Act of 1996 allowed competitive local exchange carriers / competitive access providers (CLECs) to compete with the RBOCs for local traffic. CLECs frequently partner with Tier 2/3 ISPs. The CLEC provides the access portion of the network and delivers bulk traffic to the ISP. CLECs tend to focus on business customers.

DCE—Data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. See DTE.

DTE—Data terminal equipment. Device at the user end of a user-network interface that serves as a data source, destination, or both. DTE connect to a data network through a DCE device and typically uses clocking signals generated by the DCE. See DCE.

FTP—File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

HDLC—High-level data link control. Bit-oriented synchronous data link layer protocol developed by ISO. Derived from Synchronous Data Link Control (SDLC), HDLC specified a data encapsulation method on synchronous serial linked using frame characters and checksums. See SDLC.

IP— Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.

ITU-T—International Union Telecommunication Standardization Sector. International body that develops worldwide standards for telecommunications technologies.

SDLC—Synchronous Data Link Control. Systems Network Architecture (SNA) data layer communications protocol. SDLC is bit-oriented, full-duplex serial protocol that has spawned numerous similar protocols, including HDLC and LAPB. See SNA.

SNA—Systems Network Architecture. Large, complex, feature-rich network architecture developed in the 1970s by IBM. Similar in some respects to the OSI reference model, but with a number of differences. SNA is essentially composed of seven layers: data flow control layer, data-link control layer, path control layer, physical control layer, presentation services layer, transaction service layer, and transmission control layer.

SNMP— Simple Network Management Protocol. A TCP/IP protocol built to serve as a communications channel for internetwork management operating at the application layer of the IP stack.

TCP—Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See TCP/IP and IP.

TCP/IP—Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best known protocols in the suite. See TCP and IP.

Telnet— Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connections, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

TFTP—Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network.

TL1— Translation Language 1. A widely-used management protocol for telecommunications developed by Telcordia Technologies (formerly Bellcore) under the GR-833-CORE specification.

Content Engine Network Module for Caching and Content Delivery

The Content Engine Network Module for Caching and Content Delivery feature integrates content engine (CE) functionality into branch office routers for enterprise and service provider sites. Content engine functionality provides the following benefits:

- Reduced bottlenecks and increased available bandwidth
- Offloading of a significant amount of traffic and number of TCP connections from origin servers

Transferring content engine capabilities from a router-attached appliance to an integrated network module provides the following benefits:

- Increased manageability
- Reduced complexity
- Decreased price
- Optimized performance

Feature Specifications for the Content Engine Network Module for Caching and Content Delivery

Feature History	
Release	**Modification**
12.2(11)YT	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
Supported Platforms	
Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, Cisco 3725, and Cisco 3745.	

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 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.

Contents

Prerequisites for the Content Engine Network Module for Caching and Content Delivery

- Install Cisco IOS Release 12.2(11)YT, Cisco IOS Release 12.2(13)T, or a later release.
- Install Cisco ACNS Version 4.2.3 or a later release if it is not already installed. If you have a CE network module with an installed SCSI controller expansion module, refer to the "Installing Cisco ACNS Software on a CE Network Module with a SCSI Expansion Module" section on page 414. For other types of CE network modules, refer to software installation and upgrade instructions in the documentation for the appropriate ACNS software version at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/

- Install the CE network module. Be sure that it is properly seated and that the EN (enable) and PWR (power) LEDs are lit. For information about installing CE network modules, refer to *Connecting CE Network Modules for Caching and Content Delivery*.
- For Cisco 2691, Cisco 3725, and Cisco 3745 routers only, ensure that the ROM monitor (ROMMON) version is 12.2(8r)T2 or a later version. This ROMMON version contains a fix that prevents the router from resetting all the network modules when it is reloaded.

Restrictions for the Content Engine Network Module for Caching and Content Delivery

- Cisco IOS Release 12.2(11)YT, Cisco IOS Release 12.2(13)T, or a later release is required.
- Cisco ACNS software Version 4.2.3 or a later release is required.
- The only ACNS software features supported by the CE network module are the ACNS software content engine features.
- Online insertion and removal (OIR) is supported only on Cisco 3660 and Cisco 3745 platforms.
- Transmission speed over the internal CE link is automatically negotiated between the CE interface and the Cisco IOS interface on the router side. On Cisco 2600 series and Cisco 2600XM series platforms except for the Cisco 2691, a speed of 10 Mbps is negotiated. On all other platforms, the speed of 100 Mbps is automatically negotiated.
- The maximum number of CE network modules that can be installed in a router is limited by the amount and type of power that is provided to the network module slots. Table 27 lists the maximum number of CE network modules that can be installed on different router types.

Table 27 Maximum Number of CE Network Modules per Router Type

Router Type	Number of Network Modules
Cisco 2600 series	1
Cisco 2600XM series	1
Cisco 2691	1
Cisco 3640 and Cisco 3640A	3
Cisco 3660	6
Cisco 3725	2
Cisco 3745	4

Information About the Content Engine Network Module for Caching and Content Delivery

The CE network module is specialized to run an integrated enterprise content delivery network (E-CDN) application on a Cisco Application and Content Networking System (ACNS) software platform that includes content-caching and content-delivery software.

The following concepts are helpful in understanding the CE network module:

- Cisco Content Delivery Networks
- Cisco Content Engines
- CE Network Module Hardware

Cisco Content Delivery Networks

When a Cisco E-CDN application is enabled, a combination of content engines, content routers, content services switches, and content distribution managers can be deployed to create a complete content delivery network system that includes content routing, content switching, content distribution and management, and content services, as well as content delivery. The CE network module is one element of that network. Figure 42 shows a typical E-CDN topology.

Cisco ACNS software unifies caching software and Cisco E-CDN software into a single software platform that is supported on content engines, content distribution managers, and content routers. ACNS software accelerates content delivery and optimizes bandwidth usage by caching frequently accessed content and fulfilling content requests locally rather than traversing the Internet or intranet to a distant server each time a request is made. The ACNS software cache application works in tandem with Cisco IOS routing software to handle web traffic, including user requests to view pages and graphics (objects) on World Wide Web servers—whether the traffic is internal or external to your network.

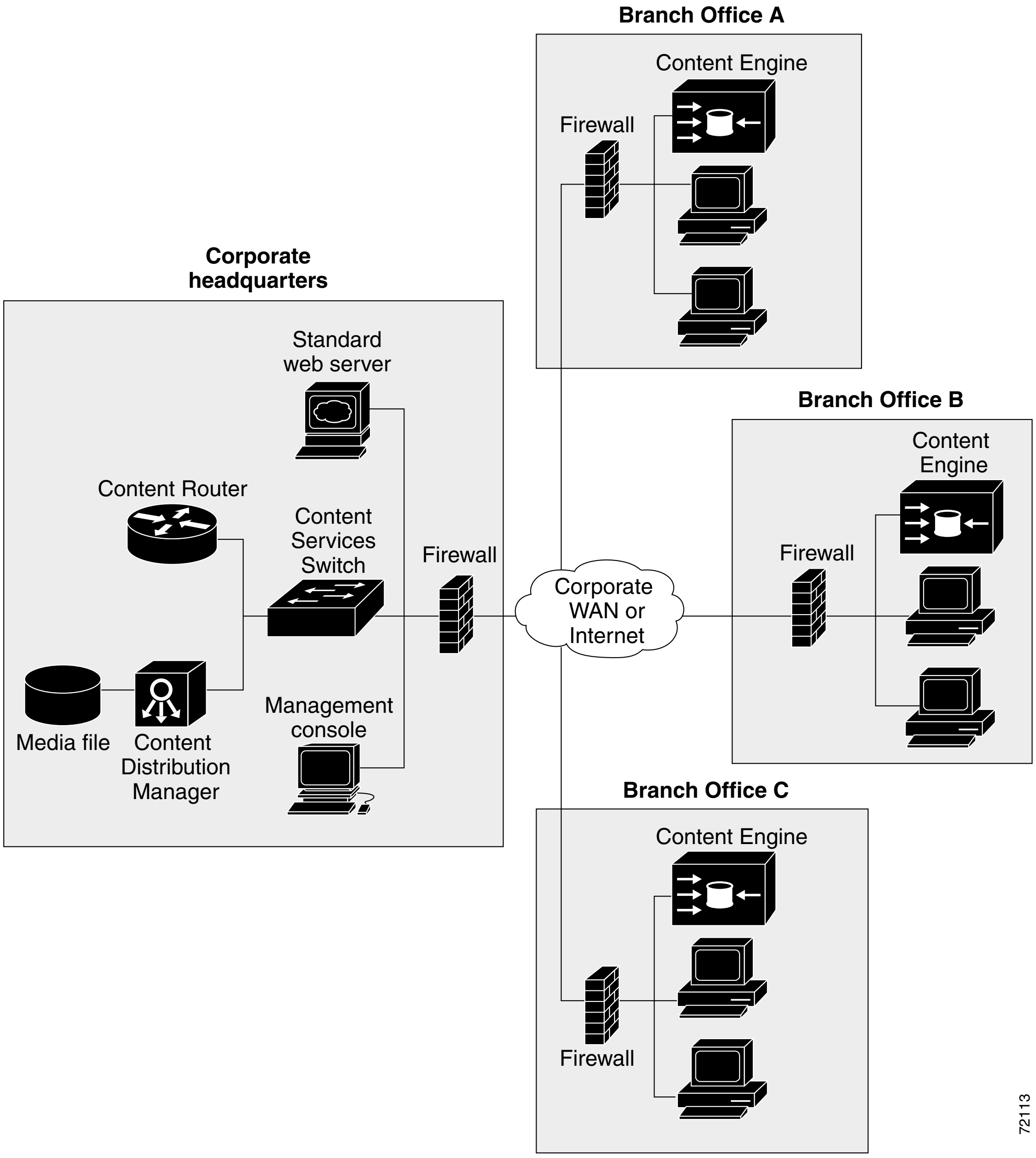
In addition to relieving WAN bottlenecks with localized caching, Cisco CEs can become the content delivery elements of a Cisco content delivery network (CDN) solution. CDN solutions enable the proactive distribution of rich media files to content engines at the network edge for local access. Primary CDN applications include e-learning, corporate communications, and software distribution. Designed for affordability and ease of installation, a CDN solution enables you to quickly deploy high-impact, high-bandwidth rich media, such as high-quality streaming video—with minimal administration.

The CE network module is completely interoperable with other CE appliances and components of an E-CDN. CE network module hardware is based on Cisco CE-507 and CE-560 architecture, uses an Intel Mobile Pentium III microprocessor, and runs under a Linux operating system.

For more information, refer to the following:

- Cisco ACNS software
- E-CDN application software within a content delivery network—*Cisco Enterprise CDN Software User Guide*
- Cisco Content Networking Technology Solution
- White paper—*The Cisco Content Delivery Network Solution for the Enterprise*
- Technical documentation—Content Delivery Networking Products

Figure 42 Cisco Enterprise Content Delivery Network Topology



Cisco Content Engines

Cisco CEs, including CE network modules, accelerate content delivery and optimize bandwidth usage in the following two ways:

- By transparently caching frequently accessed content through the Web Cache Communication Protocol (WCCP) V.2.
- By fulfilling content requests locally rather than by traversing the Internet or corporate intranet to a distant server farm each time that a request is made.

The CE leverages interception mechanisms based on Cisco IOS software to handle requests for web traffic—whether internal or external to your network. In addition, Cisco CEs can be deployed in reverse proxy mode in front of web servers to dramatically increase performance. By transparently caching inbound requests for content, CEs can offload a significant amount of traffic and number of TCP connections from origin servers. CEs dynamically distribute web content to eliminate bottlenecks and to speed access to content using this type of scenario:

1. A user (client) requests a web page from a browser.
2. A router enabled with WCCP analyzes the request and, on the basis of TCP port number, determines if it should transparently redirect the request to a CE. If so, the request is redirected to the CE.
3. If the CE has a copy of the requested object in storage, the CE sends the object to the user. Otherwise, the CE simultaneously obtains the requested object from the web server, stores a copy of the object (caches it) locally, and forwards the object to the user.
4. Subsequent requests for the same content are transparently fulfilled by the CE from its local storage.

By caching web objects in this manner, the CE can speed the satisfaction of user requests when more than one user wants to access the same object. Caching in this manner also reduces the amount of traffic between your network and the Internet, potentially improving your overall network performance and optimizing your bandwidth usage, typically resulting in WAN bandwidth savings of 25 to 60 percent.

CE Network Module Hardware

The CE network module occupies a single router slot and has the properties that are summarized in Table 28.

Table 28 CE Network Module Properties

Property	Description
Part Number	• NM-CE-BP-20G-K9 (20 GB internal storage) • NM-CE-BP-40G-K9 (40 GB internal storage) • NM-CE-BP-SCSI-K9 (SCSI connection for external storage)
Router Slot Usage	One network module slot.
Processor	Intel Mobile Pentium III, 500 MHz.
Memory	256 MB DRAM, upgradable to 512 MB.
External Compact Flash Memory	(Optional) 256 MB, Cisco part number MEM-256CF-x.x-K9=, where x.x is the version of Cisco ACNS software.

Table 28 CE Network Module (continued)Properties

Property	Description
Internal Storage	(Optional) One of the following 2.5-in. IDE drives (laptop) on an expansion module: • 20 GB, 4200 RPM • 40 GB, 5400 RPM
External Storage Connectivity	(Optional) SCSI expansion module with SCSI controller and 64-pin SCSI connector to provide connectivity to the types of external storage arrays supported by Cisco CE-507 and Cisco CE-560 content engines.
Platforms	Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, Cisco 3725, and Cisco 3745.
Power Consumption	16 watts (including IDE disk).
Expansion Modules	EM-CE-20G EM-CE-40G EM-CE-SCSI

External hardware interfaces include the following:

- An external 10/100 (Fast Ethernet) interface port that provides direct LAN connectivity. This interface has an RJ-45 connector.
- An optional SCSI expansion module that has a 64-pin SCSI connector to provide external storage array connectivity.
- An external compact Flash slot that is available to house an optional Flash memory for image recovery.

CE Network Module Operating Topologies

The CE network module can be deployed by branch office customers in one of the following topologies:

- The CE network module is directly connected to a LAN by an Ethernet switch or hub through the network module's external Fast Ethernet (FE) interface.

  Similar to situations in which a PC is connected to a LAN, the Ethernet interface on the CE network module is given an IP address from the branch office's LAN IP subnet space, which is typically configured statically using the Cisco IOS command-line interface (CLI) on the console port. One advantage of this topology is that the Fast Ethernet port on the CE network module can operate at line speed. The only communication between the router and the CE network module is in the form of keepalives or heartbeats that are processed through the internal FE ports. All caching and streaming traffic goes through the external FE port.

- The CE network module is directly connected to an Ethernet interface on the router using the internal FE interface on the CE network module.

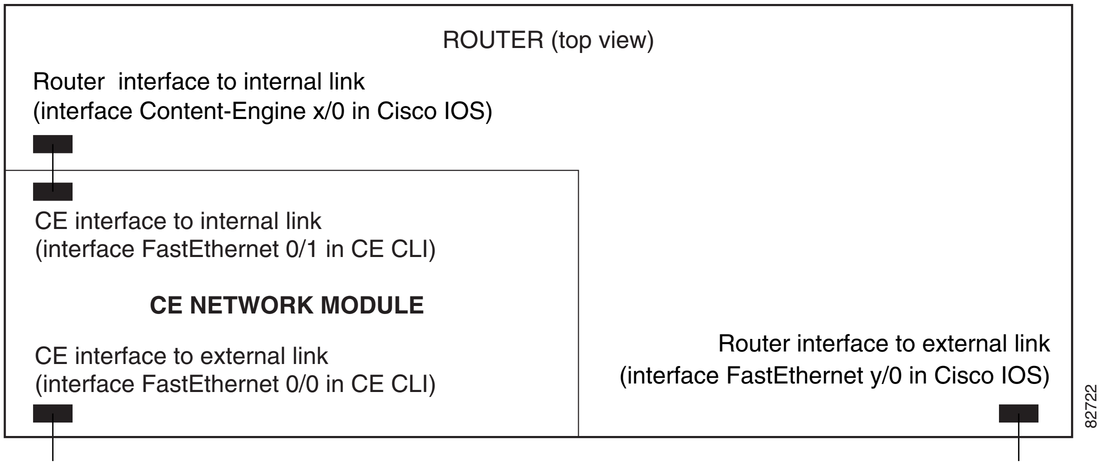
  In this topology, the Ethernet interface is given an address from an IP subnet separate from the branch office LAN subnet. All caching and streaming traffic flows through the router. The CE's performance is limited by the router's switching performance. In this scenario, streaming and caching traffic, as well as keepalive traffic, goes through internal FE ports. Caching and streaming traffic uses router resources such as CPU, SDRAM bandwidth, and backplane PCI bandwidth.

CE Network Module Interfaces

The CE network module uses three interfaces for communication, as shown in Figure 43. Two of the interfaces enable internal administrative and management traffic between the router (Cisco IOS) and the CE (Cisco ACNS software) over an internal Ethernet segment. The third interface is the external link that supports CE functionality.

Note that the interfaces within the "Router" box in Figure 43 are managed by Cisco IOS, while the interfaces within the "CE Network Module" box are managed by the CE CLI (Cisco ACNS software).

Figure 43 CE Network Module Interfaces


ROUTER (top view)
Router interface to internal link
(interface Content-Engine x/0 in Cisco IOS)
CE interface to internal link
(interface FastEthernet 0/1 in CE CLI)
CE NETWORK MODULE
CE interface to external link
(interface FastEthernet 0/0 in CE CLI)
Router interface to external link
(interface FastEthernet y/0 in Cisco IOS)
82722

The router-side interface for the internal Ethernet segment is known as interface Content-Engine in the Cisco IOS software. This interface is the only interface associated with the CE that is visible in the output of the **show interfaces** command. It provides access through the Cisco IOS software to configure the CE interfaces with IP addresses and a default gateway. The router-side internal interface is connected to the router PCI backplane and is managed by Cisco IOS CLI.

The CE side of the internal Ethernet segment is called interface FastEthernet 0/1 in the CE CLI (Cisco ACNS software). When packets are sent from the router to the CE, they are sent out from the router on interface Content-Engine and received at the CE on interface FastEthernet 0/1. When packets are sent from the CE to the router, they are sent out from the CE on interface FastEthernet 0/1 and received at the router on interface Content-Engine. The internal CE-side interface is connected to the PCI bus on the CE side, and it is managed by the CE software. Only the IP address is configured from Cisco IOS CLI. All other configurations are performed from the CE CLI or from the CE graphical user interface (GUI). Bandwidth, autosense, and duplex settings are not allowed on this interface.

The external CE interface is known as interface FastEthernet 0/0 in the CE CLI (Cisco ACNS software). This is the Ethernet port on the network module, and it supports data requests and transfers from outside sources. This link provides direct Fast Ethernet connectivity to the LAN through an RJ-45 connector. Only the IP address is configured from Cisco IOS CLI; all other configurations are performed from the CE CLI or from the CE GUI.

How to Configure and Manage the Content Engine Network Module for Caching and Content Delivery

The first configuration task for the CE network module is to define IP addresses and subnet masks for the CE network module interfaces. Because the CE network module does not have direct console access, this is a necessary first step to allow access so that you can configure ACNS software on the CE itself.

After defining IP addresses, ensure that ACNS software Version 4.2.3 or a later release is loaded on the CE network module. The type of storage memory that your CE network module employs determines how the ACNS software is installed, as follows:

- CE network modules with optional IDE expansion modules for internal storage arrive with ACNS software already installed.
- CE network modules with optional SCSI expansion modules for connecting external storage arrays arrive without ACNS software installed. You must install ACNS software by following one of the procedures in the "Installing Cisco ACNS Software on a CE Network Module with a SCSI Expansion Module" section on page 414.

Refer to the following sections for configuration, installation, and troubleshooting tasks for the CE network module. Each task in the list is identified as either required or optional.

- Configuring IP Addresses on the CE Network Module Interfaces (required)
- Opening a Console Access Session to Configure the CE Network Module (required)
- Managing the CE Network Module (optional)
- Installing Cisco ACNS Software on a CE Network Module with a SCSI Expansion Module (optional)
- Recovering a Corrupted ACNS Software Image (optional)
- Installing a Hot-Swappable CE Network Module (Cisco 3660 and Cisco 3745 Only) (optional)
- Troubleshooting Tips (optional)

Configuring IP Addresses on the CE Network Module Interfaces

In this procedure, IP addresses are configured on the three CE network module interfaces shown in Figure 43 on page 408:

- Router-side interface to the internal link
- CE interface to the internal link
- CE external interface

SUMMARY STEPS

1. **interface content-engine** *slot/unit*
2. **ip address** *router-side-ipaddr subnet-mask*
3. **service-module ip address** *ce-side-ipaddr subnet-mask*
4. **service-module external ip address** *external-ipaddr subnet-mask*
5. **service-module ip default-gateway** *gw-ipaddr*
6. **exit**

7. **exit**
8. **show running-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`interface content-engine`** *`slot`*`/`*`unit`*
	Example:
	`Router(config)# interface content-engine 4/0`
		Enters content-engine interface configuration mode for the specified interface. The arguments are as follows:
		• *slot*—Number of the router chassis slot for the network module.
		• *unit*—Number of the daughter card on the network module. For CE network modules, always use 0.

Step 2	**`ip address`** *`router-side-ipaddr subnet-mask`*
	Example:
	`Router(config-if)# ip address 172.18.12.1 255.255.255.0`
		Configures an IP address and subnet mask on the router-side interface to the internal link. The arguments are as follows:
		• *router-side-ipaddr*—IP address for the internal router-side CE interface.
		• *subnet-mask*—Subnet mask to use with the IP address.

Step 3	**`service-module ip address`** *`ce-side-ipaddr subnet-mask`*
	Example:
	`Router(config-if)# service-module ip address 172.18.12.2 255.255.255.0`
		Configures an IP address and subnet mask on the CE interface to the internal link. The arguments are as follows:
		• *ce-side-ipaddr*—IP address for the internal CE-side interface.
		• *subnet-mask*—Subnet mask to use with the IP address.

Step 4	**`service-module external ip address`** *`external-ipaddr subnet-mask`*
	Example:
	`Router(config-if)# service-module external ip address 10.3.208.190 255.255.0.0`
		Configures an IP address and subnet mask on the Fast Ethernet external interface of the CE network module. The arguments are as follows:
		• *external-ipaddr*—IP address for the external CE interface.
		• *subnet-mask*—Subnet mask to use with the IP address.

Step 5	**`service-module ip default-gateway`** *`gw-ipaddr`*
	Example:
	`Router(config-if)# service-module ip default-gateway 10.3.0.1`
		Configures an IP address for the default gateway for the CE network module. The argument is as follows:
		• *gw-ipaddr*—IP address for the default gateway.

Step 6	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits content-engine interface configuration mode.

	Command or Action	Purpose
Step 7	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 8	**show running-config** **Example:** Router# show running-config . . . ! interface Content-engine4/0 ip address 172.18.12.1 255.255.255.0 service-module external ip address 10.3.208.190 255.255.0.0 service-module ip address 172.18.12.2 255.255.255.0 service-module ip default-gateway 10.3.0.1 ! . . .	Verifies that the address configuration is correct.

Opening a Console Access Session to Configure the CE Network Module

The CE network module is a standalone content engine with its own startup and run-time configurations that are independent of the Cisco IOS configuration on the router. Although IP addresses are defined on the CE network module interfaces through the router's Cisco IOS CLI, as explained in the "Configuring IP Addresses on the CE Network Module Interfaces" section on page 409, the CE itself is configured in the same way that standalone CE appliances are configured, with a combination of CE CLI and web-based GUI. The software to configure CEs is known as Cisco Application and Content Networking System (ACNS) software.

The CE network module differs from a standalone CE appliance because it does not have an external console port. Console access to the CE network module is enabled when you issue the **service-module content-engine session** command on the router, as explained in this section, or when you initiate a Telnet connection. The lack of an external console port means that the initial boot-up configuration is possible only through the router.

When you issue the **service-module content-engine session** command, you create a console session with the CE, in which you can issue any of the CE configuration commands. After completing work in the session and exiting the CE software, you are returned to Cisco IOS CLI, where you must clear the session using the **service-module content-engine session clear** command.

Timesaver Configure IP addresses on the CE network module interfaces before opening a console access session.

SUMMARY STEPS

1. **service-module content-engine** *slot***/***unit* **session**
2. Enter ACNS configuration commands at the CE-netmodule prompt.
3. Press **Control-Shift-6**, and then press **x** to return to router configuration.
4. **service-module content-engine** *slot***/***unit* **session clear**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`service-module content-engine`** *`slot`*`/`*`unit`* **`session`**
	Example:
	`Router# service-module content-engine 4/0 session`
	`Trying 10.10.10.1, 2129 ... Open`
	`CE-netmodule con now available`
	`Press RETURN to get started!`
	`CE-netmodule> enable`
	`CE-netmodule#`
		Provides console access to the CE network module from the router CLI by initiating a reverse Telnet connection. This command places you in CE CLI configuration mode. After using the **enable** command, you are in CE CLI privileged EXEC mode.
		The reverse Telnet connection is made using the IP address of the CE interface and the terminal (TTY) line associated with the CE network module. The TTY line number is calculated using the following formula (n*32)+1, where *n* is the number of the chassis slot that contains the CE network module. In the example output provided in this step, the CE interface IP address is 10.10.10.1, and the TTY line number is 129. The number 2000 has been added to the TTY line number for the reverse Telnet session.
		The arguments are as follows:
		• *slot*—Number of the router chassis slot for the network module.
		• *unit*—Number of the daughter card on the network module. For CE network modules, always use 0.
		The CE interface must be up before you can use the **service-module content-engine session** command.
		Once a session is started, you can perform any CE configuration task. You first access the CE console in a user-level shell. The **enable** command takes you to the privileged EXEC command shell, where most commands are available.

Step 2	Enter ACNS configuration commands at the CE-netmodule prompt.	CE configuration tasks are described in documentation for the appropriate version of Cisco ACNS software at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/
Step 3	Press **Control-Shift-6**, and then press **x** to return to router configuration.	The CE session stays up until you use the **service-module content-engine session clear** command as described in Step 4. While the CE session remains up, you can use **Enter** to return to the CE session from router configuration.

	Command or Action	Purpose
Step 4	**service-module content-engine** *slot*/*unit* **session clear** **Example:** `Router# service-module content-engine 4/0 session clear`	Clears the existing CE network module configuration session. Use this command after exiting the CE module as described in Step 2. The arguments are as follows: • *slot*—Number of the router chassis slot for the network module. • *unit*—Number of the daughter card on the network module. For CE network modules, always use 0. Press **Enter** when you are asked to confirm this command.

Managing the CE Network Module

The commands in this section are used for the graceful shutdown, reset, and reload of a CE network module after it has been installed. For information on installation, refer to the following documents:

- CE network module—*Connecting CE Network Modules for Caching and Content Delivery*
- CE network module daughter card—*Installing Expansion Modules on the Cisco CE Network Module for Caching and Content Delivery*
- Network modules—*Cisco Network Modules Hardware Installation Guide*

SUMMARY STEPS

Use the following commands as necessary:

- **service-module content-engine** *slot*/*unit* **shutdown**
- **service-module content-engine** *slot*/*unit* **reset**
- **service-module content-engine** *slot*/*unit* **reload**

DETAILED STEPS

Command or Action	Purpose

service-module content-engine *slot*/*unit* **shutdown**
Example:
`Router# service-module content-engine 1/0 shutdown`
`Shutdown is used for Online removal of Service Module.`
`Do you want to proceed with shutdown?[confirm]`
`Use service module reset command to recover from shutdown.`
	Performs a graceful halt of the CE network module operating system so that the CE disks are not corrupted. Used when removing or replacing a hot-swappable CE network module during online insertion and removal (OIR). The arguments are as follows:
	• *slot*—Number of the router chassis slot for the network module.
	• *unit*—Number of the daughter card on the network module. For CE network modules, always use 0.
	At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Command or Action	Purpose

service-module content-engine *slot*/*unit* **reset**
 	
Example:
`Router# service-module content-engine 1/0 reset`
 	
`Use reset only to recover from shutdown or failed state`
`Warning: May lose data on the hard disc!`
`Do you want to reset?[confirm]`
	Performs a hardware reset of the CE network module. The arguments are as follows:
	• *slot*—Number of the router chassis slot for the network module.
	• *unit*—Number of the daughter card on the network module. For CE network modules, always use 0.
	At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

service-module content-engine *slot*/*unit* **reload**
 	
Example:
`Router# service-module content-engine 1/0 reload`
 	
`Do you want to proceed with reload?[confirm]`
	Performs a graceful halt and reload of the CE network module operating system. The arguments are as follows:
	• *slot*—Number of the router chassis slot for the network module.
	• *unit*—Number of the daughter card on the network module. For CE network modules, always use 0.
	At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Installing Cisco ACNS Software on a CE Network Module with a SCSI Expansion Module

A Cisco CE network module with an installed SCSI controller expansion module does not ship with installed ACNS software. If you have this type of CE network module, you also require an external storage array to hold the ACNS software.

Before using the CE network module, you need to install an external storage array and the Cisco ACNS software. ACNS software is installed by one of the following methods:

- From a CD-ROM—Download the software from the CD-ROM to a local FTP server. The local FTP server must be accessible to the router with the CE network module. Follow the instructions in the "Installing Cisco ACNS Software from a CD-ROM or from Cisco.com" section on page 414.
- From Cisco.com—Download the ACNS software from the Cisco Software Center at http://www.cisco.com/kobayashi/sw-center/sw-content.shtml to a local FTP server. The local FTP server must be accessible to the router with the CE network module. Follow the instructions in the "Installing Cisco ACNS Software from a CD-ROM or from Cisco.com" section on page 414.
- From a compact Flash card—Follow the instructions in the "Installing Cisco ACNS Software from Compact Flash" section on page 418.

Installing Cisco ACNS Software from a CD-ROM or from Cisco.com

To perform the Cisco ACNS software installation from a CD-ROM or from Cisco.com, you need a local FTP server that can be reached from the router that contains the CE network module. The local FTP server should be configured with a valid username and password.

The external storage array is also installed during this procedure.

Note In addition to the ACNS x.x.x image, the CD-ROM contains special upgrade and downgrade images, meta files, manifest samples, and so forth. These are not required for installation, but may be useful if you are using certain features of ACNS.

SUMMARY STEPS

1. Download to a local FTP server the Cisco ACNS software image.
2. **show disks** or **show disks details**
3. Attach the external storage array to the Cisco content engine network module.
4. **reload** or **service-module content-engine reload**
5. Configure the CE network module for IP address and default gateway.
6. **show disks** or **show disks details**
7. **disk recover**
8. **copy ftp install** {*hostname* | *ip-address*} *remotefiledir remotefilename*
9. **reload** or **service-module content-engine reload**
10. Configure the Cisco ACNS software as required.

DETAILED STEPS

Step 1 Download to a local FTP server the Cisco ACNS software image. You can use the image from either of these locations:

- The CD-ROM that accompanied the CE network module—Copy the ACNS-x.x.x-K9.bin software file, which is located in the root directory. ACNS-x.x.x-K9.bin is the generic form for the Cisco ACNS file name. For example, Cisco ACNS software version 4.2.3 has the software file name ACNS-4.2.3-K9.bin.
- The Cisco Software Center at http://www.cisco.com/kobayashi/sw-center/sw-content.shtml — Select the appropriate version of Cisco ACNS software and follow the prompts to download the ACNS software image.

Step 2 Use the **show disks** command or the **show disks details** command in CE CLI privileged EXEC mode to establish a baseline value for CE disk usage. The output of these commands establish a baseline value for the amount of disk usage or the number of disks detected, respectively. This step must be completed before you attach the external storage array. Later, in Step 6 of this procedure, you verify that the software detects the external storage array by comparing this output to the output from the same command after you have attached the external storage array.

Note Before performing this step, make sure that you have used the **ip address** command under the content-engine interface to define an IP address for the router-side interface to the internal link and that the content-engine interface is in an up state. The **ip address** command is explained in Step 2 of the "Configuring IP Addresses on the CE Network Module Interfaces" section on page 409.

The following example shows how to enter CE CLI privileged EXEC mode for the CE network module in slot 4 and then shows the two commands that you can use to establish baseline disk usage. An example of the output from the two commands is shown in Step 6.

```
Router# service-module content-engine 4/0 session

Trying 10.10.10.1, 2129 ... Open
CE-netmodule con now available
Press RETURN to get started!
CE-netmodule> enable
Password:

CE-netmodule# show disks

CE-netmodule# show disks details
```

Step 3 Attach the external storage array to the Cisco content engine network module. For information on attaching an external storage array, see the *Cisco Storage Array 6 Installation and Configuration Guide* and the hardware documents in the "Additional References" section on page 428.

Step 4 Restart the network module using either of the following commands:

- **reload**—Use this command from CE CLI privileged EXEC mode.

  ```
  CE-netmodule# reload
  ```

- **service-module content-engine reload**—Use this command from router CLI privileged EXEC mode.

  ```
  Router# service-module content-engine 4/0 reload
  Do you want to proceed with reload?[confirm]
  ```

Step 5 Configure the network module for IP address and default gateway, using Cisco IOS CE interface configuration mode on the router, as explained in the "Configuring IP Addresses on the CE Network Module Interfaces" section on page 409.

Step 6 Confirm that the external storage array is detected by the network module by using either the **show disks** command or the **show disks details** command, as explained here:

- Enter the **show disks** command in CE CLI privileged EXEC mode. The command output displays the file systems that are found on the network module. These file systems can exist on a single disk or can span multiple disks. You confirm the detection of the external storage array by noting whether the total disk space on all file systems has increased from the baseline that you noted in Step 2. The following example shows output from the **show disks** command:

  ```
  CE-netmodule# show disks

  SYSFS     0.0GB      0.0%
  CFS       0.0GB      0.0%
  MEDIAFS   0.0GB      0.0%
  ECDNFS    0.0GB      0.0%
  FREE    113.7GB    100.0%
  ```

- Enter the **show disks details** command in CE CLI privileged EXEC mode. The command output provides an entry for each disk detected. If the external storage array is detected, the number of entries in the **show disks details** command output increases from the number in the output that you saw when you used the commands in Step 2. The following example shows output from the **show disks details** command:

```
CE-netmodule# show disks details

disk00:Normal          (h00 c00 i08 100)    17364MB( 17.0GB)
        System use:              3317MB(  3.2GB)
        FREE:                   14046MB( 13.7GB)
disk01:Normal          (h00 c00 i09 100)    17366MB( 17.0GB)
        disk01/00:SYSFS         17365MB( 17.0GB) mounted at /local1
        FREE:                       0MB(  0.0GB)
disk02:Normal          (h00 c00 i10 100)    17366MB( 17.0GB)
        disk02/00:SYSFS         17365MB( 17.0GB) mounted at /local2
        FREE:                       0MB(  0.0GB)
disk03:Normal          (h00 c00 i11 100)    17366MB( 17.0GB)
        disk03/00:SYSFS         17365MB( 17.0GB) mounted at /local3
        FREE:                       0MB(  0.0GB)
disk04:Normal          (h00 c00 i11 100)    17366MB( 17.0GB)
        disk03/00:SYSFS         17365MB( 17.0GB) mounted at /local4
        FREE:                       0MB(  0.0GB)
disk05:Normal          (h00 c00 i13 100)    17366MB( 17.0GB)
        disk05/00:SYSFS         17365MB( 17.0GB) mounted at /local5
        FREE:                       0MB(  0.0GB)
```

If the external storage array is not detected by the network module, verify that the SCSI cables are connected and that the external storage array is operational. For more information on troubleshooting the external storage array, refer to the *Cisco Storage Array 6 Installation and Configuration Guide*.

Step 7 In CE CLI privileged EXEC mode, enter the **disk recover** command to create disk partitions on the external storage array for use by the network module.

```
CE-netmodule# disk recover
```

Step 8 In CE CLI privileged EXEC mode, enter the **copy ftp install** {*hostname* | *ip-address*} *remotefiledir remotefilename* command to download the Cisco ACNS software image from the FTP server to the external storage array and to the onboard Strata Flash memory on the network module. In the following example, the FTP server is server4, the directory is /images, and the image name is acns_file:

```
CE-netmodule# copy ftp install server4 /images acns_file
```

Step 9 Restart the network module as described in Step 4 of this procedure.

Step 10 Configure the Cisco ACNS software as required. For more information, refer to documentation for the appropriate version of Cisco ACNS software at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/

Installing Cisco ACNS Software from Compact Flash

If you do not have an FTP server available in the network or if the CE network module does not have network connectivity, you can install the ACNS software image from an external compact Flash card, Cisco part number MEM-256CF-x.x-K9=, where x.x is the Cisco ACNS software version.

SUMMARY STEPS

1. Insert the compact Flash card in the compact Flash slot on the front of the network module.
2. **reload** or **service-module content-engine reload**
3. After the CE network module has booted up, enter CE CLI privileged EXEC mode and list the files in compact Flash memory.
   a. **service-module content-engine** *slot***/***unit* **session**
   b. **enable**
   c. **cd flash**
   d. **dir**
4. **copy compactflash install** *image-name*
5. **reload** or **service-module content-engine reload**
6. Configure the CE with the Cisco ACNS software.

DETAILED STEPS

Step 1 Insert the compact Flash card in the compact Flash slot on the front of the network module.

Step 2 Restart the CE network module using either of the following commands:

- Use the **reload** command from CE CLI privileged EXEC mode.

```
CE-netmodule# reload
```

- Use the **service-module content-engine reload** command from router CLI privileged EXEC mode.

```
Router# service-module content-engine 4/0 reload

Do you want to proceed with reload?[confirm]
```

Step 3 After the CE network module has booted up, enter CE CLI privileged EXEC mode and list the files in compact Flash memory, using the following commands:

a. **service-module content-engine** *slot***/***unit* **session**
b. **enable**
c. **cd flash**
d. **dir**

```
Router# service-module content-engine 4/0 session

Trying 10.10.10.1, 2129 ... Open
CE-netmodule con now available
Press RETURN to get started!
CE-netmodule> enable
Password:
CE-netmodule# cd flash1
CE-netmodule# dir
```

The **dir** command displays the list of files in the compact Flash memory. The following example shows the output from a **dir** command.

```
CE-netmodule# dir
      size          time of last change             name
--------------  -------------------------          -----------
      12290784  Mon Jan  7 03:22:38 1980           sys422.img
     105990784  Mon Jan  7 03:22:38 1980           acns422.img
```

Step 4 Copy the Cisco ACNS software image to the CE network module by using the following command from CE CLI privileged EXEC mode. Substitute the actual image name from your **dir** command output for the file name “acns4xx.img” in the following example.

```
CE-netmodule# copy compactflash install acns4xx.img
```

Step 5 Restart the network module as described in Step 2 of this procedure.

Step 6 Configure the CE with the Cisco ACNS software. For more information, refer to the appropriate version of Cisco ACNS software at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/.

Recovering a Corrupted ACNS Software Image

An ACNS software image can become corrupted if there is a power failure or other interruption during an operation in which the image is being written to the CE network module’s onboard StrataFlash memory, such as during an ACNS software installation or upgrade.

If the ACNS software image on the CE network module’s onboard StrataFlash memory is corrupted, the network module boots up using a special rescue image that is also located on the onboard StrataFlash memory. The rescue image serves a limited purpose, which is simply to download a fresh Flash component of the ACNS software image and write it to the onboard StrataFlash memory. The rescue image can download this Flash component either from an FTP server on the network or from an external compact Flash card that is installed locally.

If you are going to download the Flash component from an FTP server on the network, the Flash component must first be downloaded to an FTP server from a CD-ROM or from Cisco.com over the network. This procedure and the procedure to download the image from the FTP server to the onboard Flash memory are the same as those described in the “Installing Cisco ACNS Software from a CD-ROM or from Cisco.com” section on page 414.

If you do not have an FTP server available in the network or if the network module does not have network connectivity, you can recover the ACNS software image from a special external compact Flash card, Cisco part number MEM-256CF-x.x-K9=, where x.x is the Cisco ACNS software version number.

SUMMARY STEPS

1. Insert the compact Flash card in the compact Flash slot on the front of the network module.
2. Type **4** to reboot the system.
3. Type **2** to read the image from the compact Flash and write it to the onboard StrataFlash memory.
4. Enter the directory name for the image file on the external compact Flash card.
5. Enter the filename for the image file on the external compact Flash card.
6. Type **yes** to write the image.

7. Type **yes** to reload.
8. Configure ACNS software on the network module.

DETAILED STEPS

Step 1 When a failure occurs in the ACNS software image, the CE network module automatically enters rescue mode during its bootup procedure and the following messages are displayed.

Insert the compact Flash card in the compact Flash slot on the front of the network module.

```
Freeing initrd memory:208k freed
VFS:Mounted root (ext2 filesystem).
Freeing unused kernel memory:448k freed

This is the rescue image.  The purpose of this software is to let
you install a new system image onto your system's boot flash
device.  This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has
been invoked by the bootloader if it discovered that your system image
in flash had been corrupted.

You now have the following options.

  1.  Download an image from the network and install it to flash

  2.  Insert a DOS formatted compact flash with a good system
      image on it, and install this image to flash. (The
      system must be rebooted to detect the compact flash).

  3.  Display diagnostic information about this system

  4.  Reboot the system

enter choice:
```

Step 2 Type **4** to reboot the system so that the system detects the compact Flash card you installed in Step 1.

Step 3 After the system reboots, the rescue mode messages are displayed again. At the “enter choice” prompt, type **2** to read the image from the compact Flash and write it to the onboard StrataFlash memory.

Step 4 At the next prompt, enter the directory name for the image file on the external compact Flash card. In the example below, the image file is found in the root directory (/) on the compact Flash.

```
Please enter the directory containing the image file on the compact flash:
[Enter directory on compact flash (e.g. /)]: /
```

Step 5 At the next prompt, enter the filename for the image file on the external compact Flash card. The filename has the format ACNS-x.x.x-K9.sysimg, where x.x.x is the ACNS version number. In the following example, the version is ACNS 5.0.3 and the image is named ACNS-5.0.3-K9.sysimg:

```
Please enter the file name of the system image file on the compact flash:
[Enter filename on compact flash]: ACNS-5.0.3-K9.sysimg
```

Step 6 The system provides feedback as it reads the file and then asks you to write the image to the onboard Flash memory. Type **yes** to write the image.

```
Trying to access the file //ACNS-5.0.3-K9.sysimg...
Read 12290784 byte image file
A new system image has been read from compact flash.
You should write it to system flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
yes
```

Step 7 After the ACNS software has been written to the CE network module's onboard Flash memory, the system will ask if you want to reload the network module. Type **yes** to reload.

Step 8 After the reload is complete, you can continue to configure ACNS software on the network module. Previous ACNS software configurations are saved.

Installing a Hot-Swappable CE Network Module (Cisco 3660 and Cisco 3745 Only)

Some Cisco modular access routers allow you to replace network modules without switching off the router or affecting the operation of other interfaces. This feature is often called *hot-swapping* or *online insertion and removal (OIR).* Hot-swapping of network modules provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Note OIR is supported only on Cisco 3660 and Cisco 3745 platforms.

Caution Unlike other network modules, CE network modules use hard disks. Online removal of disks without proper shutdown can result in file system corruption and might render the disk unusable. The operating system on the CE network module must be shut down in an orderly fashion before the network module is removed.

Caution Cisco routers support hot-swapping with similar modules only. If you remove a network module, install another module exactly like it in its place.

For a description of informational messages and error messages that may appear on the console during this procedure, refer to the hardware installation guide for your type of router.

SUMMARY STEPS

1. **service-module content-engine session**
2. **copy running-config tftp** *tftp-server-address filename*
3. **Control-Shift-6**, followed by **x**
4. **service-module content-engine** *slot***/***unit* **session clear**
5. **service-module content-engine** *slot***/***unit* **shutdown**
6. Shut down the CE interface.
   a. **interface content-engine** *slot***/***unit*
   b. **shutdown**
   c. **exit**
7. Unplug all network interface cables from the CE network module.
8. Loosen the two captive screws holding the CE network module in the chassis slot.

9. Slide the CE network module out of the slot.
10. Align the replacement CE network module with the guides in the chassis slot, and slide it gently into the slot.
11. Push the module into place until you feel its edge connector mate securely with the connector on the backplane.
12. Reconnect the network interface cables previously removed in Step 7.
13. Check that the network module LEDs are lit and that the Power and Enable LEDs on the front panel are also lit.
14. **service-module content-engine** *slot*/*unit* **session**
15. **copy tftp running-config** *tftp-server-address filename*
16. **Control-Shift-6**, followed by **x**
17. **service-module content-engine** *slot*/*unit* **session clear**

DETAILED STEPS

Step 1 Initiate a CE network module console access session using the **service-module content-engine session** command. The following example shows the starting of a session for the CE network module in slot 4.

```
Router# service-module content-engine 4/0 session

Trying 10.10.10.1, 2129 ... Open

CE-netmodule con now available

Press RETURN to get started!

CE-netmodule> enable
Password:

CE-netmodule#
```

Step 2 Save the CE running configuration using the following command from CE CLI privileged EXEC mode.

```
CE-netmodule# copy running-config tftp //server12/configs/rtr11-confg
```

Step 3 Exit the CE network module console access session by pressing **Control-Shift-6**, followed by **x**.

Step 4 On the router, clear the CE console access session using the following command.

```
Router# service-module content-engine 4/0 session clear
```

Step 5 Perform a graceful halt of the CE network module disk drive using the following command.

```
Router# service-module content-engine 4/0 shutdown
```

Step 6 Shut down the CE interface.

```
Router(config)# interface content-engine 4/0
Router(config-if)# shutdown
Router(config-if)# exit
```

Step 7 Unplug all network interface cables from the CE network module.

Step 8 Loosen the two captive screws holding the CE network module in the chassis slot.

Step 9 Slide the CE network module out of the slot.

Step 10 Align the replacement CE network module with the guides in the chassis slot, and slide it gently into the slot.

Note If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow.

Step 11 Push the module into place until you feel its edge connector mate securely with the connector on the backplane.

Step 12 Reconnect the network interface cables previously removed in Step 7.

Step 13 Check that the network module LEDs are lit and that the Power and Enable LEDs on the front panel are also lit. This inspection ensures that connections are secure and that the new unit is operational.

Step 14 Initiate a CE network module console access session using the following command.

```
Router# service-module content-engine 4/0 session

Trying 10.10.10.1, 2129 ... Open

CE-netmodule con now available
Press RETURN to get started!

CE-netmodule> enable
Password:

CE-netmodule#
```

Step 15 Restore the CE running configuration by using the following command from CE CLI privileged EXEC mode.

```
CE-netmodule# copy tftp running-config //server12/configs/rtr11-confg
```

Step 16 Exit the CE network module console access session by pressing **Control-Shift-6**, followed by **x**.

Step 17 On the router, clear the CE console access session using the following command.

```
Router# service-module content-engine 1/0 session clear
```

Troubleshooting Tips

To diagnose problems with CE network module operation, use the commands and actions in this section.

- Display configured commands using the **show running-config** command. Make sure that a new interface called *Content-Engine* is displayed and that the IP addresses listed for the CE are correct. The Content-Engine interface is the router-side interface for the internal Ethernet segment between the router and the CE, and it is the only CE interface that is displayed in the output of the **show running-config** command. The other two CE interfaces appear as “service-modules” under the Content-Engine interface. For more information on CE interfaces, refer to the “CE Network Module Interfaces” section on page 408.
- Display software version information using the **show version** command. The following output example shows a CE network module and its terminal line listed in the interface information section:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.2(11)YT, RELEASE SOFTWARE (fc1)
```

```
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 12-Sep-02 21:34 by axpo
Image text-base: 0x80008098, data-base: 0x818AF44C

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

router-2621 uptime is 10 minutes
System returned to ROM by power-on
System image file is "flash:c2600-is-mz"

cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory.
Processor board ID JAD051516TV (4151953086)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
1 terminal line(s)
1 cisco content engine(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x0
```

- Display the basic interface configuration and the number of packets transmitted, output rate, and related information using the **show interfaces content-engine** command.
- Display information for controllers that are associated with the CE network module using the **show controllers content-engine** command.
- Display the status of the content engine, as well as the hardware configuration, software version, and related information, using the **service-module content-engine status** command.
- Display hardware installed on the router using the **show diag** command. The following output example shows a CE network module in router slot 1:

```
Router# show diag 1

Slot 1:
        Content Engine Port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time unknown
        EEPROM contents at hardware discovery:
        Hardware Revision        : 1.0
        Top Assy. Part Number    : 800-20382-01
        Board Revision           : A0
        Deviation Number         : 0-0
        Fab Version              : 02
        PCB Serial Number        : JAB060605C4
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 03 81 41 01 00 C0 46 03 20 00 4F 9E 01
          0x10: 42 41 30 80 00 00 00 00 02 02 C1 8B 4A 41 42 30
          0x20: 36 30 36 30 35 43 34 03 00 81 00 00 00 00 04 00
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
20GB IDE Disc Daughter Card
Hardware Revision         : 1.0
Top Assy. Part Number     : 800-20520-01
Board Revision            : A0
Deviation Number          : 0-0
Fab Version               : 02
PCB Serial Number         : JAB060605A5
RMA Test History          : 00
RMA Number                : 0-0-0-0
RMA History               : 00

EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF 40 03 83 41 01 00 C0 46 03 20 00 50 28 01
  0x10: 42 41 30 80 00 00 00 00 02 02 C1 8B 4A 41 42 30
  0x20: 36 30 36 30 35 41 35 03 00 81 00 00 00 00 04 00
  0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

- After exiting a CE console access session, remember to use the **service-module content-engine session clear** command to terminate the session.
- Check LEDs that are associated with the CE network module. The link activity LED should light up whenever packets are being transmitted through the port.
- If Cisco Discovery Protocol (CDP) is enabled in the CE network module, use the **debug cdp packet** command to see the CDP packets going across the interfaces every 60 seconds, which is the default. Use the **show cdp neighbor** command to see all the Cisco devices that have CDP enabled and that are in the same segment.
- Enable the **debug scp all** command to check the communication between the Cisco IOS software and the CE:

```
Router# debug scp all

*Mar  1 00:28:34.371: scp-tx: SA:0F/01 DA:01/01 Op:0012 Sq:0024 Ln:0004 I:00
*Mar  1 00:28:34.371: 000: 02 5A 00 00                                  .Z..
*Mar  1 00:28:34.371: scp-rx: SA:01/01 DA:0F/01 Op:0012 Sq:0024 Ln:0004 I:01
*Mar  1 00:28:34.371: 000: 02 5A 00 00                                      .Z..
```

Configuration Examples for the Content Engine Network Module for Caching and Content Delivery

This section provides the following configuration examples:

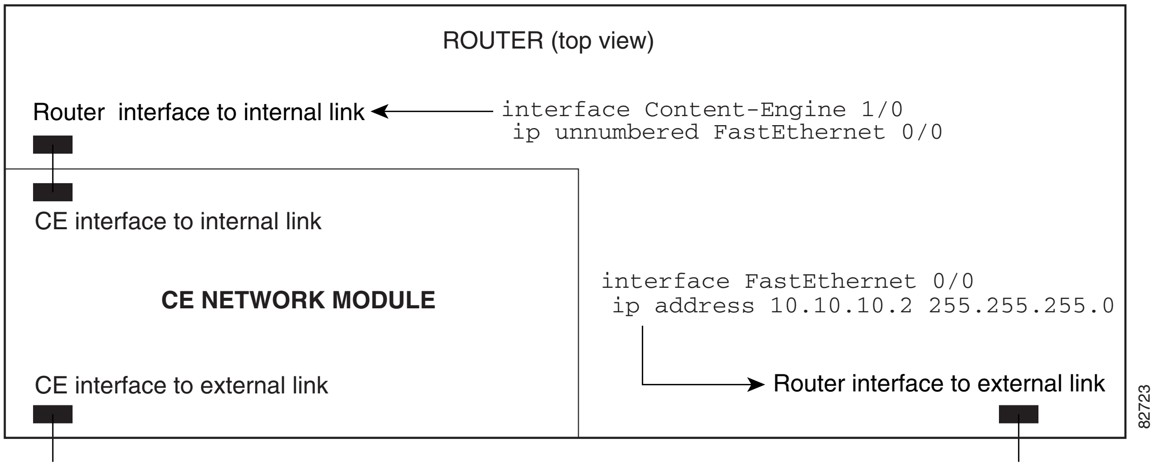
- Unnumbered IP Address Example
- Three IP Address Example

Note IP addresses and host names used in examples are fictitious.

Unnumbered IP Address Example

Figure 44 shows how the CE interfaces are configured using the unnumbered IP address method. In this example, the router interface to the internal router-CE link is configured using the **ip unnumbered** command to save IP address space. No new subnet needs to be defined for the internal network between the router and the CE. This configuration makes the CE interface that is pointing toward the Cisco IOS software an extension of the Fast Ethernet interface 0/0 of the router, which has an IP address of 10.10.10.2. When this method is used, a static IP route must be defined.

Figure 44 Unnumbered IP Address Example

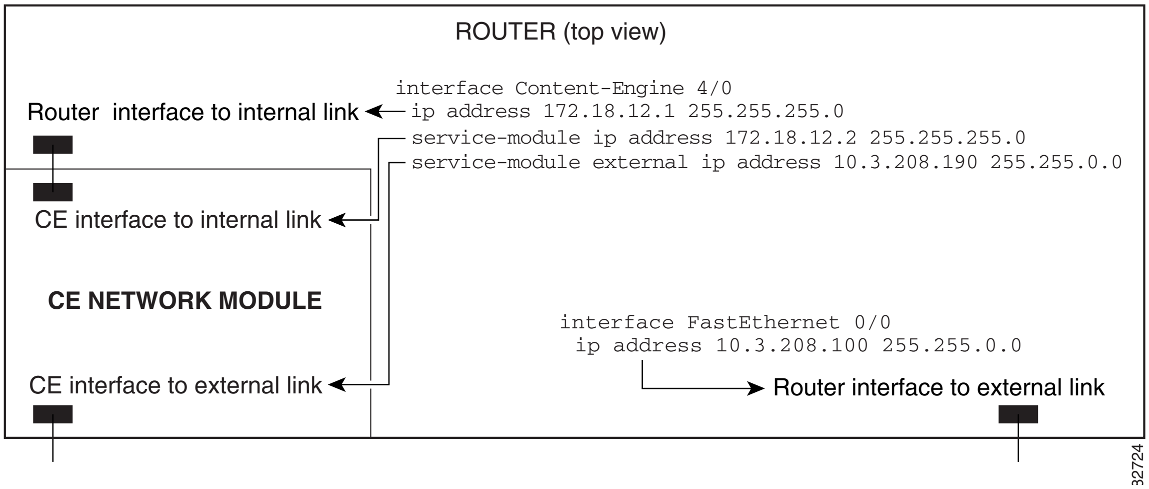

ROUTER (top view)
Router interface to internal link
interface Content-Engine 1/0
ip unnumbered FastEthernet 0/0
CE interface to internal link
CE NETWORK MODULE
interface FastEthernet 0/0
ip address 10.10.10.2 255.255.255.0
CE interface to external link
Router interface to external link
82723

```
.
.
.
!
interface Content-Engine 1/0
 ip unnumbered FastEthernet 0/0
 service-module ip address 10.10.10.10 255.255.255.0
 service-module external ip address 172.18.12.20 255.255.255.0
 service-module ip default-gateway 10.10.10.2
!
ip route 10.10.10.10 255.255.255.255 Content-Engine 1/0
!
.
.
.
```

Three IP Address Example

Figure 45 shows the configuration for the three IP address method. In this example, both the CE interface to the internal router-CE link and the router interface to the same link are on the 172.18.12.0/24 subnet. The external port of the CE network module is in the 10.3.0.0/16 subnet. Notice that there is no connection between the internal router interface to the CE and the external router interface in this configuration.

Figure 45 Three IP Address Example



ROUTER (top view)
Router interface to internal link
CE interface to internal link
CE NETWORK MODULE
CE interface to external link
Router interface to external link
32724

```
interface Content-Engine 4/0
 ip address 172.18.12.1 255.255.255.0
 service-module ip address 172.18.12.2 255.255.255.0
 service-module external ip address 10.3.208.190 255.255.0.0
```

```
interface FastEthernet 0/0
 ip address 10.3.208.100 255.255.0.0
```

```
.
.
.
!
interface Content-Engine 4/0
 ip address 172.18.12.1 255.255.255.0
 service-module ip address 172.18.12.2 255.255.255.0
 service-module external ip address 10.3.208.190 255.255.0.0
 service-module ip default-gateway 10.3.0.1
!
.
.
```

Additional References

For additional information related to the Content Engine Network Module for Caching and Content Delivery, refer to the following references:

Related Documents

Related Topic	Document Title
Related content delivery products	Content Delivery Networking Products
Cisco ACNS software	Refer to documentation for the appropriate version of Cisco ACNS software at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/
E-CDN application software within a content delivery network	*Cisco CDN Software Enterprise User Guide*
Cisco Content Delivery Networks (white paper)	*The Cisco Content Delivery Network Solution for the Enterprise*
Cisco Content Networking technologies (web site)	*Cisco Content Networking Technology Solution*
Overview and installation of Content Delivery Networking products	*Cisco Content Delivery Networking Products Getting Started Guide*
Installing CE network modules	*Connecting CE Network Modules for Caching and Content Delivery*
Installing CE network module expansion modules	*Installing Expansion Modules on the Cisco CE Network Module for Caching and Content Delivery*
Installing CE network module memory modules	*Installing SODIMM Memory Modules in Cisco Network Modules for Caching and Content Delivery*
Installing network modules	*Cisco Network Modules Hardware Installation Guide*
Installing storage arrays	*Cisco Storage Array 6 Installation and Configuration Guide*
Cisco 2600 series	Cisco 2600 series product documentation
Cisco 3600 series	Cisco 3600 series product documentation
Cisco 3700 series	Cisco 3700 series product documentation

Standards

Standards[1]	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

[1] Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
• CISCO-CONTENT-ENGINE-MIB • CISCO-ENTITY-ASSET-MIB • ENTITY-MIB • MIB-2 • CDP-MIB	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

[1] Not all supported MIBs are listed.

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

RFCs[1]	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified 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, tools, and lots more. 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.

New Commands

- **service-module content-engine reload**
- **service-module content-engine reset**
- **service-module content-engine session**
- **service-module content-engine session clear**
- **service-module content-engine shutdown**
- **service-module content-engine status**
- **service-module external ip address**
- **service-module ip address**
- **service-module ip default-gateway**
- **show controllers content-engine**
- **show interfaces content-engine**

Modified Command

- **interface**

Glossary

ACNS—Cisco Application and Content Networking System. ACNS is a software platform that unifies the Cisco cache software and Cisco enterprise content delivery network (E-CDN) software into a single software platform. ACNS software allows you to access caching application features and E-CDN application features from a single software base. ACNS software is supported on content engines, content distribution managers, and content routers.

CDM—Cisco Content Distribution Manager. Management program that provides a browser-based user interface to configure and monitor content engines and content routers and to control and manage content switching, content distribution and delivery, and content services.

CDN—content delivery network. Content delivery networks help accelerate the delivery of advanced content by deploying five key components: content switching, content routing, content edge nodes, content distribution and management, and intelligent network services. Content edge nodes are content engines that are typically placed in the branch office, like the CE network module.

CE—content engine. Edge appliance for delivering live or on-demand streaming media and other rich file formats to the desktop.

E-CDN—enterprise content delivery network. Enterprise CDNs (also known as intranet CDNs) apply caching and multicasting technology in a corporate LAN/WAN environment to distribute video and other content-rich files in ways that help minimize WAN bottlenecks, while taking advantage of the relatively abundant bandwidth of the LANs close to users.

WCCP—Web Cache Communication Protocol. Developed by Cisco Systems, WCCP specifies interactions between one or more routers (or Layer 3 switches) and one or more web caches. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a group of routers. The selected traffic is redirected to a group of web caches with the aim of optimizing resource usage and lowering response times.

Digital J1 Voice Interface Card

Feature History

Release	Modification
12.2(8)T	This feature was introduced on the Cisco 2600 and Cisco 3600 series.

This document describes the Digital J1 Voice Interface Card feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

Feature Overview

The J1 interface card provides the proper interface for directly connecting Cisco multiservice access routers to Private Branch Exchanges (PBXs) throughout Japan that use a J1 interface (2.048 Mbps TDM interface). This interface card supports 30 voice channels per port.

It provides the software and hardware features required to connect to over 80percent of the PBXs within Japan that use digital interfaces. This new J1 voice interface card (VIC) provides a TTC JJ-20.11 compliant interface between high-density voice network modules (NM-HDV) and a Japanese PBX.

The digital J1 card provides a single-port line interface in a VIC form factor. It is specifically designed to conform to the TTC JJ-20.10-12 standards that define the interface between a PBX and time-division multiplexer (TDM).

Figure 1 shows the earlier solution offered to customers in Japan. A J1/T1 adapter box installed between the PBX and router provides the translation between J1 using coded mark inversion (CMI) line coding at a bit rate of 2.048 Mbps and a T1 line using either alternate mark inversion (AMI) or B8ZS line coding at a bit rate of 1.544 Mbps. Note that with this solution, only 24 channels are supported, instead of the full 30 channels of the J1 interface.

Figure 46 Solution without J1 Interface Card

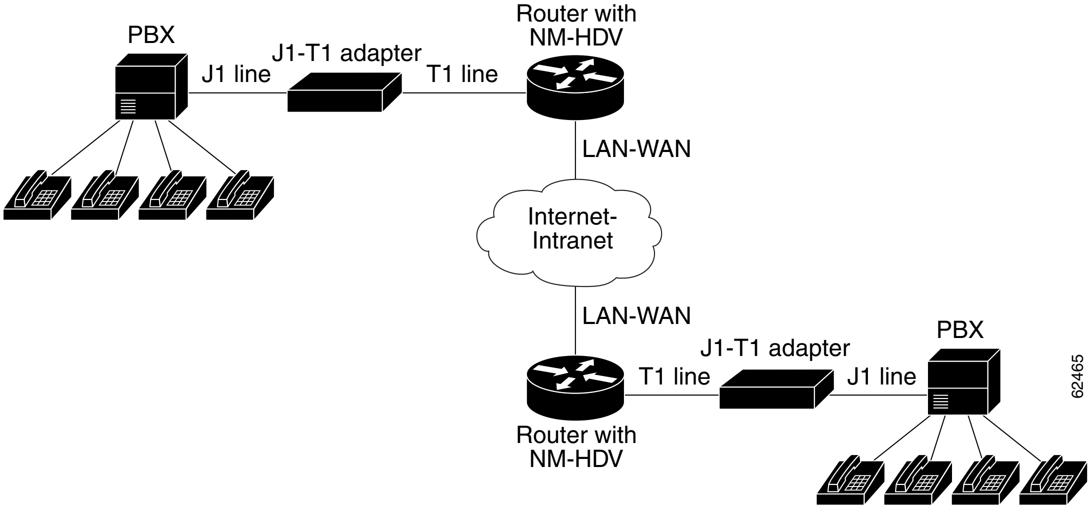
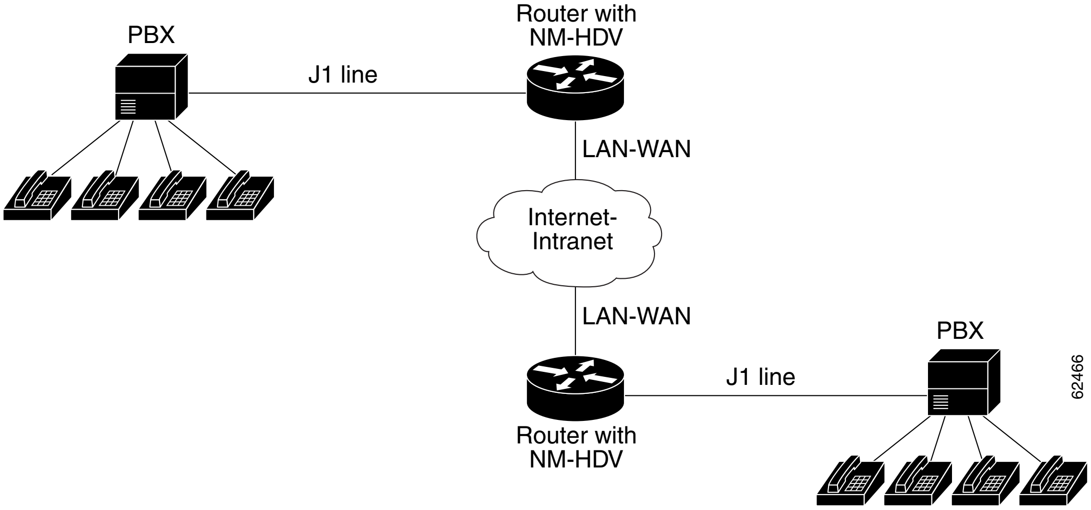


Figure 2 shows the solution using the J1 interface card. The interface is now between J1 and the VIC's time division multiplex access (TDMA) bus. Note that now all 30 channels of the J1 interface are supported.

Figure 47 Solution with J1 Interface Card



Benefits

- Support for Media Gateway Control Protocol (MGCP), H.248, H.323 (versions 1, 2, and 3), Session Initiation Protocol (SIP) and Cisco Call Manager (with Cisco IP phones) in association with VoIP, VoFR, and VoATM.
- Provides Alarm Indication Signal (AIS) alarm signaling per TTC JJ-20.11.
- Delivers the same performance as the existing 30 channel E1 NM-HDV.
- Allows one to enable and disable individual DS0's or channels.

Restrictions

- Voice only applications.
- Separate clock output not supported.
- Alarm relay output not supported.
- Per channel loopback not supported.
- Voice ports on the J1 interface cannot be configured using network management software. They can only be configured manually.

Related Documents

- *Installing and Configuring 1-Port J1 Voice Interface Cards*
- *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2

Supported Platforms

- Cisco 2600 series
- Cisco 3600 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

- General specification TTC JJ-20.10
- TTC interface specification TTC JJ-20.11
- TTC Signaling specification TTC JJ-20.12 (E&M wink start, wink immediate, and DTMF only).

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

None

Prerequisites

- Cisco IOS Release 12.2(8)T or later release.

Configuration Tasks

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional:

- Configuring the J1 Controller (required)
- Configuring Channel-Associated Signaling (optional)
- Configuring the Clock Source (optional)
- Configuring Loopback (optional)
- Configuring Transparent Common Channel Signaling for a Clear-Channel Codec (optional)
- Verifying Configuration (optional)

Configuring the J1 Controller

Use the following procedure to configure the J1 controller.

	Command	Purpose
Step 5	`Router# configure terminal`	Enters global configuration mode.
Step 6	`Router(config)# controller j1 slot/port`	Selects the J1 controller to configure. *slot/port*—Backplane slot number and port number on the controller.

Configuring Channel-Associated Signaling

Configure the DS0 groups on the J1 controller for voice applications. The J1 controller supports the E&M wink start and E&M immediate channel associated signaling (CAS) protocols for the voice ports.

The following parameters have default values for the J1 interface:

- The companding type is ulaw.
- The CP tone is set to JP.

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# controller j1 slot/port`	Selects the J1 controller to configure and enters controller configuration mode. This example configures a J1 controller in slot 1 and port 0.

	Command	Purpose
Step 3	Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** *signaling-type* **service** *service-type*	Command defines the j1 1/0 for use by compressed voice calls and the signaling method the router uses to connect to the PBX. **Note** This step shows the basic syntax and signaling types available with the **ds0-group** command. For the complete syntax, see the *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2. The keywords and arguments are as follows: • *ds0-group-no*—Specifies the DS0 group number. • **timeslots** *timeslot-list*—Specifies the DS0 time slot range of values from 1 to 31 for J1 interfaces. Time slot 16 is reserved for signaling. • **type** *signaling-type*—(optional) Specifies the signaling type to be applied to the selected group. The options are as follows: – **e&m-delay-dial**—Specifies that the originating endpoint sends an off-hook signal and then and waits for an off-hook signal followed by an on-hook signal from the destination. – **e&m-immediate-start**—Specifies no specific off-hook and on-hook signaling. – **e&m-wink-start—**Specifies that the originating endpoint sends an off-hook signal and waits for a wink signal from the destination. – **none**—Specifies null signaling for external call control.
Step 4	Router(config-controller)# **exit**	Exits to global configuration mode. Return to Step 2 if your router has more than one J1 controller that you need to configure.

Configuring the Clock Source

Use the following procedure to configure the clock source for a J1 controller.

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`controller j1 1/0`**	Selects the J1 controller to configure and enters controller configuration mode. This example configures a J1 controller in slot 1 and port 0.
Step 3	`Router(config-controller)#` **`clock source`** `{`**`line`** `|`**`internal`**`}`	Specifies the clock source, either internal or line. • **line**—The controller recovers external clock from the line and provides the recovered clock to the internal (system) clock generator. The line value is the default clock source. • **internal**—The controller synchronizes itself to the internal (system) clock.
Step 4	`Router(config-controller)#` **`exit`**	Exits to global configuration mode. Return to Step 2 if your router has more than one J1 controller that you need to configure.

Configuring Loopback

Use the following procedure to configure the loopback for testing a J1 controller.

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode. You have entered global configuration mode when the prompt changes to `Router(config)#`.
Step 2	`Router(config)#` **`controller j1 1/0`**	Selects the J1 controller to configure and enters controller configuration mode. This example configures a J1 controller in slot 1 and port 0.
Step 3	`Router(config-controller)#` **`loopback`** `{`**`local`** `|` **`line`** `|` **`isolation`**`}`	Sets the loopback method for testing the J1 interface. • **local**—Places the interface into local loopback mode. • **line**—Places the interface into external loopback mode at the line level • **isolation**—Both local and line loopback.
Step 4	`Router(config-controller)#` **`exit`**	Exits to global configuration mode.

Configuring Transparent Common Channel Signaling for a Clear-Channel Codec

Use the following procedure to configure transparent common channel signaling (T-CCS).

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **controller j1** *slot/port*	Selects the J1 controller to configure. *slot/port*—Backplane slot number and port number on the controller.
Step 3	Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** *ext-sig*	This command defines the j1 0 for use by compressed voice calls and the signaling method the router uses to connect to the PBX. **Note** This step shows the basic syntax and signaling types available with the **ds0-group** command. For the complete syntax, see the *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2. The keywords and arguments are as follows: • *ds0-group-no*—Specifies the DS0 group number. • **timeslots** *timeslot-list*—Specifies the DS0 time slot range of values from 1 to 31 for J1 interfaces. Time slot 16 is reserved for signaling. • **type** *ext-sig***—**(optional) The signaling method selection for type depends on the connection that you are making:The external signaling interface specifies that the signaling traffic comes from an outside source.
Step 4	Router(config-controller)# **no shutdown**	Activates the controller.
Step 5	Router(config-controller)# **exit**	Exits controller configuration mode.
Step 6	Router(config)# **dial-peer voice** *number* **pots**	Enters dial-peer configuration mode and define a local dial peer that connects to the plain old telephone service (POTS) network. The value of *number* is one or more digits identifying the dial peer. Valid entries are from 1 through 2147483647. The **pots** argument indicates a peer using a basic telephone service.

	Command	Purpose
Step 7	`Router(config-dialpeer)# destination-pattern string [T]`	Configures the dial peer's destination pattern so that the system can reconcile dialed digits with a telephone number. The value of *string* is a series of digits that specify the E.164 or private dialing plan phone number. Valid entries are the digits 0 through 9 and the letters A through D. The plus symbol (+) is not valid. You can enter the following special characters: • The star character (*) that appears on standard touch-tone dial pads can be in any dial string—but not as a leading character (for example, *650). • The period (.) acts as a wildcard character. • Use the comma (,) only in prefixes, the comma inserts a one-second pause. When the timer (T) character is included at the end of the destination pattern, the system collects dialed digits as they are entered—until the interdigit timer expires (10 seconds, by default)—or the user dials the termination of end-of-dialing key (default is #). **Note** The timer character must be a capital T.
Step 8	`Router(config-dialpeer)# port slot/port:ds0-group-no`	Associates the dial peer with a specific logical interface. The value of *slot* is the router location where the voice module is installed. Valid entries are from 0 through 3. The value of *port* indicates the voice interface card location. Valid entries are 0 or 1. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s.
Step 9	`Router(config-dialpeer)# exit`	Exit dial-peer configuration mode to complete the POTS dial-peer configuration.
Step 10	`Router(config)# dial-peer voice number voip`	Enters dial-peer configuration mode and defines a remote VoIP dial peer. The value of *number* is one or more digits identifying the dial peer. Valid entries are from 1 through 2147483647. The **voip** argument indicates a VoIP peer using voice encapsulation on the IP network.
Step 11	`Router(config-dialpeer)# codec clear-channel`	Set codec option to **clear-channel** to use the clear channel codec.

	Command	Purpose
Step 12	`Router(config-dialpeer)#` **`vad`**	(optional) This setting is enabled by default. It activates voice activity detection (VAD) which allows the system to reduce unnecessary voice transmissions caused by unfiltered background noise.
Step 13	`Router(config-dialpeer)#` **`destination-pattern`** *`string`* `[`**`T`**`]`	Configures the dial peer's destination pattern so that the system can reconcile dialed digits with a telephone number. The value of *string* is a series of digits that specify the E.164 or private dialing plan phone number. Valid entries are the digits 0 through 9 and the letters A through D. The plus symbol (+) is not valid. You can enter the following special characters: • The star character (*) that appears on standard touch-tone dial pads can be in any dial string—but not as a leading character (for example, *650). • The period (.) acts as a wildcard character. • Use the comma (,) only in prefixes, the comma inserts a one-second pause. When the timer (T) character is included at the end of the destination pattern, the system collects dialed digits as they are entered—until the interdigit timer expires (10 seconds, by default)—or the user dials the termination of end-of-dialing key (default is #). **Note** The timer character must be a capital T.
Step 14	`Router(config-dialpeer)#` **`session target`** `{`**`ipv4:`***`destination-address`* | **`dns:[$s$.`** | **`$d$.`** | **`$e$.`** | **`$u$.]`** *`host-name`*`}`	Configure the IP session target for the dial peer. The **ipv4:***destination-address* parameter indicates IP address of the dial peer. The **dns:***host-name* parameter indicates that the domain name server will resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device. There are also wildcards available for defining domain names with the keyword by using source, destination, and dialed information in the host name. For complete command syntax information, see *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2
Step 15	`Router(config-dialpeer)#` **`exit`**	Exit dial peer configuration mode for the VoIP dial-peer configuration.

Verifying Configuration

To verify that J1 controller is configured correctly, enter the **show running-config** privileged EXEC command to display the command settings for the router, as shown in the "Configuration Examples" section.

Troubleshooting Tips

Diagnostics and Fault Isolation

Three digital loopback modes are possible for diagnostics and fault isolation.

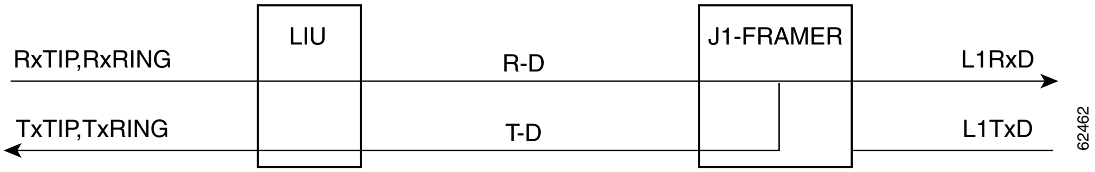
Loopback Modes

The J1 Framer has three loopback modes that are initiated through software control; line loopback, local loopback, and isolation loopback. Line loopback loops the received signal (R-D) from the PBX to the transmit going back to the PBX. Local loopback loops the transmitted signal (T-D) from the host to the receive going back to the host. Isolation loopback routes PBX and TDM generated traffic back to their respective sources. (Tx=transmit interface; Rx=receive interface;
Tip / Ring leads carry audio between the signaling unit and the trunking circuit).

- Line Loopback: To place the controller into line loopback, use the following command in controller configuration mode.

Command	Purpose
loopback line	Line loopback loops the receiver inputs to the transmitter outputs. The receive path is not affected by the activation of this loopback.

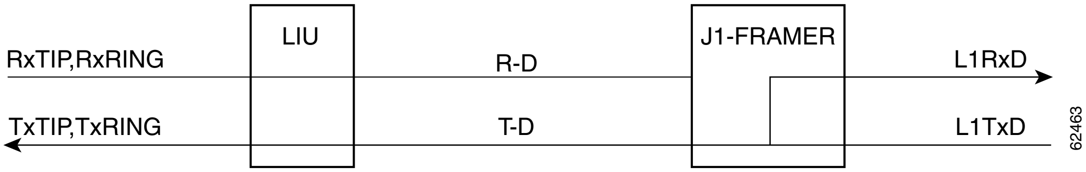
Figure 48 Line Loopback



- Local Loopback: To place the controller into local loopback, use the following command in controller configuration mode. Use the **no** form of this command to turn off the loopback. The command should only be used for testing purposes.

Command	Purpose
loopback local	Local loopback loops the transmit line encoder outputs to the receive line encoder inputs. The transmit path is not affected by the activation of this loopback.

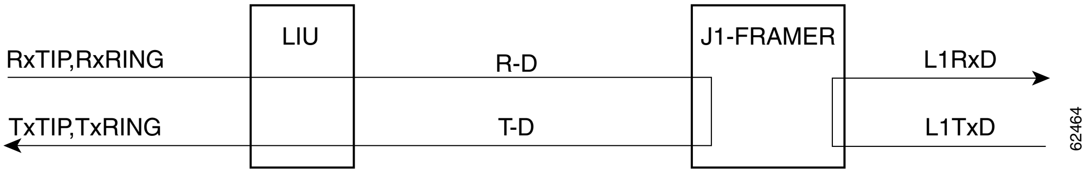
Figure 49 Local Loopback



- Isolation Loopback: To place the controller into line loopback, use the following command in controller configuration mode.

Command	Purpose
loopback isolation	Both line and local loopback are turned on.

Figure 50 Isolation Loopback



Monitoring and Maintaining the J1 Controller

To monitor and maintain the J1 controller use the following privileged EXEC command.

Command	Purpose
`Router#` **`show controllers j1`** *slot/port*	Displays statistics for the J1 link.
`Router#` **`show dial-peer voice`**	Displays configuration information for dial peers.

Configuration Examples

The following displays the screen output using the **show running-config** command. Then it is broken down into specific examples:

- Controller (J1) Example
- Channel-Associated Signaling Example
- Clock Source Example
- Loopback Example
- Transparent Common Channel Signaling for a Clear-Channel Codec Example

```
Router#show run
Building configuration...

Current configuration :2023 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname kmm-3660-1
!
boot system tftp /tftpboot/kmenon/c3660-is-mz 223.255.254.254
enable password lab
!
voice-card 1
!
voice-card 3
!
voice-card 4
!
ip subnet-zero
!
!
!
!
!
voice service pots
!
!
!
!
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller J1 1/0
 clock source line
!
controller E1 3/0
!
controller E1 3/1
!
controller T1 4/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 24
!
controller T1 4/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 24
!
!
!
!
interface Multilink1
 ip address 30.30.30.1 255.255.255.0
 keepalive 1
 no cdp enable
 ppp multilink
 no ppp multilink fragmentation
 multilink-group 1
```

```
!
interface FastEthernet0/0
 ip address 1.7.29.1 255.255.0.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 1.8.0.1 255.255.0.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Serial4/0:0
 no ip address
 encapsulation ppp
 no fair-queue
 no cdp enable
 ppp multilink
 multilink-group 1
!
interface Serial4/1:0
 no ip address
 encapsulation ppp
 no fair-queue
 no cdp enable
 ppp multilink
 multilink-group 1
!
ip default-gateway 1.7.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 1.9.0.1 255.255.255.255 30.30.30.2
ip route 223.255.254.254 255.255.255.255 1.7.0.1
no ip http server
ip pim bidir-enable
!
!
!
snmp-server engineID local 00000009020000044D0EF520
snmp-server packetsize 4096
!
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 destination-pattern 88
!
dial-peer voice 20 voip
 destination-pattern 3050
 session target ipv4:1.8.0.2
 codec clear-channel
!
dial-peer voice 77 pots
 destination-pattern 77
!
dial-peer voice 100 voip
```

```
 incoming called-number 100
 destination-pattern 100
 session target ipv4:1.8.0.2
 no vad
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end
```

Controller (J1) Example

The following example shows the Cisco IOS interface card in slot 4, port 0 of a Cisco 3660 configured as a J1 controller:

```
controller J1 4/0
```

Channel-Associated Signaling Example

The following example shows the DS0 groups on the J1 controller.

```
controller J1 4/0
 clock source line
 ds0-group 1 timeslots 1-15,17-31 type e&m-wink-start
```

Clock Source Example

The following example shows the J1 controller clock source is configured to line, where the controller recovers external clock from the line and provides the recovered clock to the internal (system) clock generator.

```
controller J1 3/0
 clock source line
```

Loopback Example

The following example shows the loopback method for testing the J1 controller is set at the line level.

```
controller J1 3/0
 clock source line
 loopback line
```

Transparent Common Channel Signaling for a Clear-Channel Codec Example

The following example shows the codec option set to clear-channel.

```
dial-peer voice 20 voip
 destination-pattern 3050
 session target ipv4:1.8.0.2
 codec clear-channel
```

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.

New Commands

- **show controllers j1**

Modified Commands

- **clock source (controller j1)**
- **controller (j1)**
- **ds0-group (controller j1)**
- **loopback (controller j1)**
- **microcode reload controller (j1)**

Glossary

AIS—alarm indication s22ignal. 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.

AMI—alternate mark inversion. Line-code type used on T1 and E1 circuits.

CAS—channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.

CCS—common channel signaling. Signaling system used in telephone networks that separates signaling information from user data. A specified channel is exclusively designated to carry signaling information for all other channels in the system.

CMI—coded mark inversion. ITU-T line coding technique specified for STS-3c transmissions.

codec—In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.

E&M—recEive and transMit (or ear and mouth). Trunking arrangement generally used for two-way switch-to-switch or switch-to-network connections. Cisco's analog E&M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines). E&M is also available on E1 and T1 digital interfaces.

FPGA—field programmable gate array.

J1 framer—A functional block within the VIC FPGA which works in tandem with the LIUs to perform the J1 framing, monitoring and loopback functions.

LIU—line interface unit.

MGCP—Media Gateway Control Protocol. A merging of the IPDC and SGCP protocols.

OOF—Out Of Frame. A designation for a condition defined as either the network or the DTE equipment sensing an error in framing bits.

NM-HDV—High-Density Voice network modules.

SIP—session initiation protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.

TDM—time division multiplex. Technique in which information from multiple channels can be allocated bandwidth on a single wire based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

TDMA—time division multiplex access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval ("slot" or "slice") for the transmission of each channel, that is, the channels take turns to use the link. Some kind of periodic synchronizing signal or distinguishing identifier usually is required so that the receiver can tell which channel is which.

VIC—voice interface card. Connects the system to either the PSTN or to a PBX.

VoATM—Voice over ATM. Voice over ATM enables a router to carry voice traffic (for example, telephone calls and faxes) over an ATM network. When sending voice traffic over ATM, the voice traffic is encapsulated using a special AAL5 encapsulation for multiplexed voice.

VoFR—Voice over Frame Relay. Voice over Frame Relay enables a router to carry voice traffic (for example, telephone calls and faxes) over a Frame Relay network. When sending voice traffic over Frame Relay, the voice traffic is segmented and encapsulated for transit across the Frame Relay network using FRF.12 encapsulation.

VoIP—Voice over IP. The ability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality.

Multichannel STM-1 Port Adapter

Feature History

12.0(14)S	This feature was introduced for the Cisco 7500 series on Cisco IOS Release 12.0(14)S.
12.1(7)E	This feature was integrated into Cisco IOS Release 12.1(7)E. Support for this feature was added to Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T for Cisco Cisco 7200 and Cisco 7500 series routers.

This feature module describes the multichannel STM-1 port adapter (PA-MC-STM-1) in Cisco IOS Release 12.2(8)T and includes the following sections:

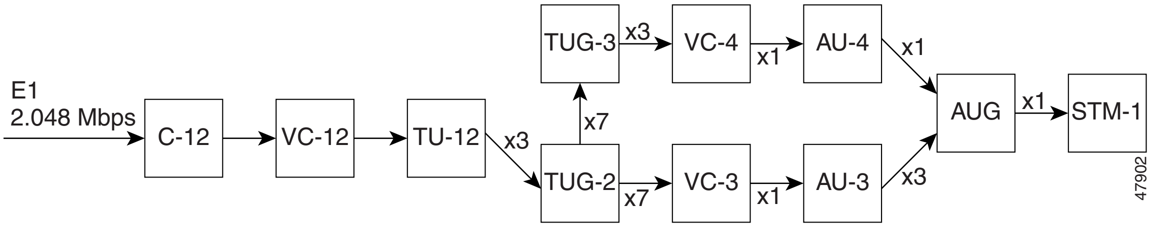
Feature Overview

The PA-MC-STM-1 is a high-speed, single-port multichannel STM-1 port adapter. You can configure the PA-MC-STM-1 as a multichannel E1/E0 STM-1 port. The PA-MC-STM-1 can be configured into 63 individual E1 links. Each E1 link can carry a single channel at full or fractional rates, or be broken down into multiple DS0 or nx64 Kbps rates. The PA-MC-STM-1 supports up to three TUG-3/AU-3 transport slots numbered 1 through 3. You can configure each TUG-3/AU-3 to carry 21 SDH TU-12s. Each SDH TU-12 is capable of carrying a channelized E1 frame, which can be unchannelized to nx64-Kbps time slots.

PA-MC-STM-1 Multiplexing Hierarchy

Figure 51 illustrates the synchronous digital hierarchy (SDH) multiplexing structure supported on the PA-MC-STM-1. The PA-MC-STM-1 multiplexing structure is a subset of that defined in ITU-T G.707. At the lowest level, containers (Cs) are input into virtual containers (VCs) with stuffing bits to create a uniform VC payload with a common bit-rate, ready for synchronous multiplexing. The VCs are then aligned into tributary units (TUs) where pointer processing operations are implemented. This allows the TUs to be multiplexed into TU groups (TUGs). Three TU-12s can be multiplexed into one TUG-2.

Figure 51 PA-STM-1 Multiplexing Structure



The TUGs are then multiplexed into higher-level VCs, which in turn are multiplexed into administrative units (AUs).The AUs are then multiplexed into an AU group (AUG), and the final payload from the AUG is then multiplexed into the Synchronous Transport Module (STM).

Benefits

The PA-MC-STM-1 port adapter provides the following benefits:

- High-density IP aggregation
- Reduction in provisioning costs
- Improved cable management
- Easier scaling of services
- Improved network availability

Restrictions

The PA-MC-STM-1 does not support the following:

- VIP2
- More than 256 logical channel groups per PA-MC-STM-1
- Channel-associated signaling (CAS) for voice channels
- E1 Facility Data Link (FDL)
- E3 and subrate E3

Related Features and Technologies

- PA-MC-T3
- PA-MC-E3

Related Documents

- *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.2
- *Cisco IOS Wide-Area Networking Command Reference,* Release 12.2
- *Multichannel STM-1 Port Adapter Installation and Configuration*
- *Multichannel STM-1 Port Adapter for the Cisco 7500 Series Router*

Supported Platforms

- 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 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

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

- CSA C22.2, No. 950
- ITU-T G.704
- ITU-T G.706
- ITU-TG.707
- ITU-T O.151
- ITU-T O.152
- ITU-T O.153
- FCC Part 15, class A
- FCC Part 68
- UL1950 3rd Edition

MIBs

No new or modified MIBs are supported by this feature.

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

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

RFCs

- RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types*
- RFC 1595, *Definitions of Managed Objects for the SONET/SDH Interface Type*

Note Because E1 FDL is not supported by the PA-MC-STM-1, the far-end statistics and control groups defined by RFC 1406 are not available.

Prerequisites

The PA-MC-STM-1 requires a VIP4-80 installed in a Cisco 7500 series router.

Configuration Tasks

See the following sections for configuration tasks for the PA-MC-STM-1. Each task in the list indicates if the task is optional or required.

- Configuring the SONET Controller (required)
- Configuring an AU-3 (required)
- Configuring a TUG-3 (required)
- Configuring a Channel Group on an E1 of an AU-3 (required)

- Configuring a Channel Group on an E1 of a TUG-3 (required)
- Configuring an E1 Line Mapped to an AU-3 (required)
- Configuring an E1 Line Mapped to a TUG-3 (required)
- Verifying the Configuration (optional)

Configuring the SONET Controller

To configure the SONET controller, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode and specifies that the console terminal is the source of the configuration subcommands.

Step 2	**Cisco 7200 series**
	`Router(config)# controller sonet slot/port`
	Cisco 7500 series
	`Router(config)# controller sonet slot/port-adapter/port`
		Selects a port of a PA-MC-STM-1 and enters controller configuration mode.

Step 3	`Router(config-controller)# framing {sonet | sdh}`	Configures the framing mode of the PA-MC-STM-1 to SONET or SDH. **sdh**—Selects SDH framing. SDH is the ITU standards equivalent of SONET. **sonet**—Selects SONET framing. SONET is the default.
Step 4	`Router(config-controller)# clock source {internal | line}`	Configures the clock source used by the SONET controller. • **internal**—The clocking source is obtained from the port adapter line. • **line**—The clocking source is obtained from the network. Network clocking source is the default.
Step 5	`Router(config-controller)# loopback {local | network}`	Enables loopback mode on a SONET controller. • **local**—Data is looped from the transmit path to the receive path allowing diagnostics to send data to itself without relying on any external connections. • **network**—Data is looped from the external port to the transmit port and back out the external port. No loopback enabled is the default.
Step 6	`Router(config-controller)# description string`	Specifies up to 80 characters of text describing the SONET controller. No description is the default.

Configuring an AU-3

Each of the administrative unit group (AUGs) and tributary unit group (TUGs) of a PA-MC-STM-1 can be configured to carry a set of E1 links that are mapped into TU-12s. To configure the AUG mapping to AU-3, use the following commands beginning in global configuration mode:

	Command	Purpose

Step 1	**Cisco 7200 series**
	`Router(config)# controller sonet slot/port`
	Cisco 7500 series
	`Router(config)# controller sonet slot/port-adapter/port`
		Enters SONET controller configuration mode.

Step 2	`Router(config-controller)# framing sdh`	Configures the framing mode to SDH.
Step 3	`Router(config-controller)# aug mapping au-3`	Maps the AUG to AU-3 with the following muxing, alignment, and mapping: C-12 <-->VC-12 <--> TU-12<--> TUG-2 <--> VC-3 <--> AU-3 <--> AUG
Step 4	`Router(config-controller)# au-3 au-3-number`	Specifies the AU-3 number to configure:. • *au-3-number*—A number in the range of 1 to 3.
Step 5	`Router(config-ctrlr-au3)# mode c-12`	Specifies the mode of operation of the AU-3. • **c-12**—The AU-3 is divided into 21 TU-12s, each carrying an E1.
Step 6	`Router(config-ctrlr-au3)# idle pattern pattern`	Configures the idle pattern that is to be transmitted for unused time slots on all E1 lines of an AU-3. • *pattern*—Number in the range 0x0 to 0xFF (hexadecimal) or 0 to 225 (decimal).

Configuring a TUG-3

Each of the administrative unit groups (AUGs) and tributary unit groups (TUGs) of a PA-MC-STM-1 can be configured to carry a set of E1 links that are mapped into TU-12s. To configure the AUG mapping to AU-4, use the following commands beginning in global configuration mode:

	Command	Purpose

Step 1	**Cisco 7200 series**
	`Router(config)# controller sonet slot/port`
	Cisco 7500 series
	`Router(config)# controller sonet slot/port-adapter/port`
		Enters SONET controller configuration mode.

Step 2	`Router(config-controller)# framing sdh`	Configures the framing mode to SDH.

	Command	Purpose
Step 3	`Router(config-controller)# aug mapping au-4`	Maps the AUG to AU-4 with the following muxing, alignment, and mapping: C-12 <--> VC-12 <--> TU-12 <--> TUG-2 <--> TUG-3 <--> VC-4 <--> AU-4 <--> AUG
Step 4	`Router(config-controller)# au-4 au-4-number tug-3 tug-3-number`	Specifies the TUG-3 number to configure: • *au-4-number*—A number in the range of 1 to *n* where *n* is the STM level. (For the PA-MC-STM-1, *n* is always 1.) • *tug-3-number*—A number in the range of 1 to 3.
Step 5	`Router(config-ctrlr-tug3)# mode c-12`	Specifies the mode of operation of a TUG-3: • **c-12**—The TUG-3 is divided into 21 TU-12s each carrying an E1.
Step 6	`Router(config-ctrlr-tug3)# idle pattern pattern`	Configures the idle pattern that is to be transmitted for unused time slots on all E1 lines of an AU-4. • *pattern*—Number in the range 0x0 to 0xFF (hexadecimal) or 0 to 225 (decimal).

Configuring a Channel Group on an E1 of an AU-3

To configure a channel group on an E1 of an AU-3, use the following commands beginning in global configuration mode:

	Command	Purpose

Step 1	**Cisco 7200 series**
	`Router(config)# controller sonet slot/port`
	Cisco 7500 series
	`Router(config)# controller sonet slot/port-adapter/port`
		Enters SONET controller configuration mode.

Step 2	`Router(config-controller)# framing sdh`	Configures the framing mode to SDH.
Step 3	`Router(config-controller)# aug mapping au-3`	Maps the AUG to an AU-3 with the following muxing, alignment, and mapping: C-12 <-->VC-12 <--> TU-12 <--> TUG-2 <--> VC-3 <--> AU-3 <--> AUG
Step 4	`Router(config-controller)# au-3 au-3-number`	Specifies the AU-3 number to configure. • *au-3-number*—A number in the range of 1 to 3.
Step 5	`Router(config-ctrlr-au3)# mode c-12`	Specifies the mode of operation of the AU-3. • **c-12**—The AU-3 is divided into 21 TU-12s each carrying an E1.

	Command	Purpose
Step 6	Router(config-ctrlr-tug3)# **tug-2** *tug-2-number* **e1** *e1-number* **channel-group** *channel-group-number* **timeslots** *list-of-timeslots*	Creates a logical channel group on an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • **channel-group**—Defines a logical channel group to be a channelized E1 line. • *channel-group-number*—A number in the range of 0 to 30. • *list-of-timeslots*—A number in the range of 1 to 31 or a combination of subranges within 1 to 31. (Each subrange is a list of time slots that makes up the E1 line.)
	or	Use the **no** form of this command to remove a logical channel group. The default is no channel group configured on an E1 line.
	Router(config-ctrlr-tug3)# **tug-2** *tug-2-number* **e1** *e1-number* **unframed**	Creates an unframed (clear channel) logical channel group on an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3.
Step 7	Router(config-ctrlr-au3)# **exit** Router(config-controller)# **exit**	Returns to configuration mode.
Step 8	**Cisco 7200 series** Router(config)# **interface serial** *slot/port.au-3-number/tug-2-number/ e1-number:channel-group-number* **Cisco 7500 series** Router(config)# **interface serial** *slot/port-adapter/port.au-3-number/tug-2-number/ e1-number:channel-group-number*	Selects the channel group interface to configure. **Note** When an unframed (clear channel) logical channel group is configured on an E1 line, the *channel-group-number* is always 0.
Step 9	Router(config-if)# **ip address** *1.1.1.10 255.255.255.255*	Enables IP on the channel group interface.
Step 10	Router(config-if)# **encapsulation ppp**	Enables PPP on the channel group interface.

Configuring a Channel Group on an E1 of a TUG-3

To configure a channel group on an E1 of a TUG-3, use the following commands beginning in global configuration mode:

	Command	Purpose

Step 1	**Cisco 7200 series**
	`Router(config)# `**`controller sonet`** *`slot/port`*
	Cisco 7500 series
	`Router(config)# `**`controller sonet`** *`slot/port-adapter/port`*
		Enters SONET controller configuration mode.

Step 2	`Router(config-controller)# `**`framing sdh`**	Configures the framing mode to SDH.
Step 3	`Router(config-controller)# `**`aug mapping au-4`**	Maps the AUG to AU-4 with the following muxing, alignment, and mapping: C-12 <--> VC-12 <--> TU-12 <--> TUG-2 <--> TUG-3 <--> VC-4 <--> AU-4 <--> AUG
Step 4	`Router(config-controller)# `**`au-4`** *`au-4-number`* **`tug-3`** *`tug-3-number`*	Specifies the AU-4 and TUG-3 number to configure: • *au-4-number*—A number in the range of 1 to *n* where *n* is the STM level. (For the PA-MC-STM-1, *n* is always 1.) • *tug-3-number*—A number in the range of 1 to 3.
Step 5	`Router(config-ctrlr-tug3)# `**`mode c-12`**	Specifies the mode of operation of an AU-4. • **c-12**—The TUG-3 is divided into 21 TU-12s each carrying an E1.

	Command	Purpose
Step 6	Router(config-ctrlr-tug3)# **tug-2** *tug-2-number* **e1** *e1-number* **channel-group** *channel-group-number* **timeslots** *list-of-timeslots*	Creates a logical channel group on an E1 line. - *tug-2-number*—A number in the range of 1 to 7. - *e1-number*—A number in the range of 1 to 3. - **channel-group**—Defines a logical channel group to be a channelized E1 line. - *channel-group-number*—A number in the range of 0 to 30. - *list-of-timeslots*—A number in the range of 1 to 31 or a combination of subranges within 1 to 31. (Each subrange is a list of time slots that makes up the E1 line.)
	or	Use the **no** form of this command to remove a logical channel group. The default is no channel group configured on an E1 line.
	Router(config-ctrlr-tug3)# **tug-2** *tug-2-number* ***e1*** *e1-number* **unframed**	Creates an unframed (clear channel) logical channel group on an E1 line. - *tug-2-number*—A number in the range of 1 to 7. - *e1-number*—A number in the range of 1 to 3.
Step 7	Router(config-ctrlr-tug3)# **exit** Router(config-controller)# **exit**	Returns to configuration mode.
Step 8	**Cisco 7200 series** Router(config)# **interface serial** *slot/port.au-4-number/tug-3-number/tug-2-number/ e1-number:channel-group-number* **Cisco 7500 series** Router(config)# **interface serial** *slot/port-adapter/port.au-4-number/tug-3-number/tug-2-number/ e1-number:channel-group-number*	Selects the channel group interface to configure. **Note** When an unframed (clear channel) logical channel group is configured on an E1 line, the *channel-group-number* is always 0.
Step 9	Router(config-if)# **ip address** *1.1.1.10 255.255.255.255*	Enables IP on the channel group interface.
Step 10	Router(config-if)# **encapsulation ppp**	Enables PPP on the channel group interface.

Configuring an E1 Line Mapped to an AU-3

To configure an E1 line mapped to an AU-3, use the following commands beginning in global configuration mode:

	Command	Purpose

Step 1	**Cisco 7200 series**
	`Router(config)# `**`controller sonet`** *`slot/port`*
	Cisco 7500 series
	`Router(config)# `**`controller sonet`**
	`slot/port-adapter/port`
		Enters SONET controller configuration mode.

Step 2	`Router(config-controller)# `**`aug mapping au-3`**	Maps the AUG to an AU-3 with the following muxing, alignment, and mapping: C-12 <--> VC-12 <--> TU-12 <--> TUG-2 <--> VC-3 <--> AU-3 <--> AUG
Step 3	`Router(config-controller)# `**`au-3`** *`au-3-number`*	Specifies the AU-3 number to configure. • *au-3-number*—A number in the range of 1 to 3.
Step 4	`Router(config-ctrlr-au3)# `**`mode c-12`**	Specifies the mode of operation of the AU-3. • **c-12**—The AU-3 is divided into 21 TU-12s each carrying an E1.
Step 5	`Router(config-ctrlr-au3)# `**`tug-2`** *`tug-2-number`* **`e1`** *`e1-number`* **`framing`** `{`**`crc4`** `|` **`no crc4`**`}`	Specifies the type of framing used by an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • **crc4**—4-bit cyclic redundancy check. • **no crc4**—Basic framing. The default is CRC4.
Step 6	`Router(config-ctrlr-au3)# `**`tug-2`** *`tug-2-number`* **`e1`** *`e1-number`* **`clock source`** `{`**`internal`** `|` **`line`**`}`	Specifies the clock source to be used by the E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • **internal**—Specifies the PA-MC-STM-1 as the clock source. • **line**—Specifies the E1 line as the clock source. The default is E1 line clock source.
Step 7	`Router(config-ctrlr-au3)# `**`tug-2`** *`tug-2-number`* **`e1`** *`e1-number`* **`national bits`** *`pattern`*	Configures the national reserved bits for the E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • *pattern*—The national reserved bit pattern is a hexadecimal value in the range 0x0 to 0x1F (hexadecimal) or 0 to 31 (decimal). The default setting is 0x1F.

	Command	Purpose
Step 8	Router(config-ctrlr-au3)# **tug-2** *tug-2-number* **e1** *e1-number* **bert pattern** *pattern* **interval** *time*	Sends a BERT pattern on an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • *pattern* – 2^11, pseudorandom test pattern (2048 bits long) – 2^15, pseudorandom O.151 test pattern (32,768 bits long) – 2^20-O153, 2^20-1 O.153 test pattern – 2^20-QRSS, pseudorandom QRSS O.151 test pattern (1,048,575 bits long) • *time*—An interval in the range of 1 to14,400 minutes. The default is no BER test configured.
Step 9	Router(config-ctrlr-au3)# **tug-2** *tug-2-number* **e1** *e1-number* **loopback** [**local** | **network** {**line** | **payload**}]	Specifies a loopback for an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • **local**—Loops transmitted E1 output back to the router via the internal E1 framer and loops E1 output to the network via the internal E1 framer. • **network**—Loops E1 input back to the network.
Step 10	Router(config-ctrlr-au3)# **tug-2** *tug-2-number* **e1** *e1-number* **shutdown**	Shuts down an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3.

Configuring an E1 Line Mapped to a TUG-3

To configure an E1 line mapped to a TUG-3, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	**Cisco 7200 series** Router(config)# **controller sonet** *slot/port* **Cisco 7500 series** Router(config)# **controller sonet** *slot/port-adapter/port*	Enters SONET controller configuration mode.
Step 2	Router(config-controller)# **aug mapping au-4**	Maps the AUG to AU-4 with the following muxing, alignment, and mapping: C-12 <--> VC-12 <--> TU-12 <--> TUG-2 <--> TUG-3 <--> VC-4 <--> AU-4 <--> AUG

	Command	Purpose
Step 3	Router(config-controller)# **au-4** *au-4-number* **tug-3** *tug-3-number*	Specifies the AU-4 and TUG-3 number to configure: • *au-4-number*—A number in the range of 1 to *n* where *n* is the STM level. (For the PA-MC-STM-1 *n* is always 1.) • *tug-3-number*—A number in the range of 1 to 3.
Step 4	Router(config-ctrlr-tug3)# **mode c-12**	Specifies the mode of operation of a TUG-3. • **c-12**—The TUG-3 is divided into 21 TU-12s, each carrying an E1.
Step 5	Router(config-ctrlr-tug3)# **tug-2** *tug-2-number* **e1** *e1-number* **framing** {**crc4** | **no crc4**}	Specifies the type of framing used an by an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • **crc4**—4-bit cyclic redundancy check. • **no crc4**—Basic framing. The default is CRC4.
Step 6	Router(config-ctrlr-tug3)# **tug-2** *tug-2-number* **e1** *e1-number* **clock source** {**internal** | **line**}	Specifies the clock source to be used by the E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • **internal**—Specifies the PA-MC-STM-1 as the clock source. • **line**—Specifies the E1 line as the clock source. The default is E1 line clock source.
Step 7	Router(config-ctrlr-tug3)# **tug-2** *tug-2-number* **e1** *e1-number* **national bits** *pattern*	Configures the national reserved bits for the E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • *pattern*—The national reserved bit pattern is a hexadecimal value in the range 0x0 to 0x1F (hexadecimal) or 0 to 31 (decimal). The default setting is 0x1F.

	Command	Purpose
Step 8	`Router(config-ctrlr-tug3)# tug-2 tug-2-number e1 e1-number bert pattern pattern interval time`	Sends a BERT pattern on an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • *pattern* – 2^11, pseudorandom test pattern (2048 bits long) – 2^15, pseudorandom O.151 test pattern (32,768 bits long) – 2^20-O153, 2^20-1 O.153 test pattern – 2^20-QRSS, pseudorandom QRSS O.151 test pattern (1,048,575 bits long) • **interval**— An interval in the range of 1 to 14400 minutes. The default is no BER test configured.
Step 9	`Router(config-ctrlr-tug3)# tug-2 tug-2-number e1 e1-number loopback [local | network {line | payload}]`	Specifies a loopback for an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3. • **local**—Loops transmitted E1 output back to the router via the internal E1 framer and loops E1 output to the network via the internal E1 framer. • **network**—Loops E1 input back to the network.
Step 10	`Router(config-ctrlr-tug3)# tug-2 tug-2-number e1 e1-number shutdown`	Shuts down an E1 line. • *tug-2-number*—A number in the range of 1 to 7. • *e1-number*—A number in the range of 1 to 3.

Verifying the Configuration

You can verify the configuration and status of the controller by using the **show controller** commands as detailed below.

When AUG mapping is AU-4, view information about the SONET controller on a Cisco 7200 series router using the **sonet controller sonet** *slot/port* [**brief** | **tabular**] command. Use the **sonet controller sonet** *slot/port-adapter/port* [**brief** | **tabular**] command for a Cisco 7500 series router.

The following examples show sample output for a Cisco 7500 series router:

```
Router# show controller sonet 2/0/0
SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
  Applique type is Channelized Sonet/SDH
  Clock Source is Internal, AUG mapping is AU4.

Medium info:
  Type:SDH, Line Coding:NRZ, Line Type:Short SM
```

```
Regenerator Section Status:
  No alarms detected.

Multiplex Section Status:
  No alarms detected.

Higher Order Path Status:
  Path# 1 has no defects

Lower Order Path Status:
  VC-12 1/1/1/1 has no defects
  VC-12 1/1/1/2 has no defects
  VC-12 1/1/1/3 has no defects
  VC-12 1/1/2/1 has no defects
  VC-12 1/1/2/2 has no defects
  VC-12 1/1/2/3 has no defects

[display text omitted]

Data in current interval (137 seconds elapsed):
   Regenerator Section:
     0 CVs, 0 ESs, 0 SESs, 0 SEFSs
   Multiplex Section:
     0 CVs, 0 ESs, 0 SESs, 0 UASs
   Higher Order Path:
     Path# 1: 0 CVs, 0 ESs, 0 SESs, 0 UASs
   Lower Order Path:
     VC-12 1/1/1/1: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     VC-12 1/1/1/2: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     VC-12 1/1/1/3: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     VC-12 1/1/2/1: 0 CVs, 0 ESs, 0 SESs, 0 UASs
[display text omitted]

SONET 2/0/0   E1   1/1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  Data in current interval (137 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
SONET 2/0/0   E1   1/1/1/2 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  Data in current interval (137 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
[display text omitted]

Router# show controller sonet 2/0/0 brief
SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
  Applique type is Channelized Sonet/SDH
  Clock Source is Internal, AUG mapping is AU4.

Medium info:
  Type:SDH, Line Coding:NRZ, Line Type:Short SM

Regenerator Section Status:
  No alarms detected.
```

```
Multiplex Section Status:
  No alarms detected.

Higher Order Path Status:
  Path# 1 has no defects

Lower Order Path Status:
  VC-12 1/1/1/1 has no defects
  VC-12 1/1/1/2 has no defects
  VC-12 1/1/1/3 has no defects
  VC-12 1/1/2/1 has no defects
  VC-12 1/1/2/2 has no defects
  VC-12 1/1/2/3 has no defects
[display text omitted]

SONET 2/0/0   E1   1/1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
SONET 2/0/0   E1   1/1/1/2 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
SONET 2/0/0   E1   1/1/1/3 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
[display text omitted]

Router# show controller sonet 2/0/0 tabular
SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
  Applique type is Channelized Sonet/SDH
  Clock Source is Internal, AUG mapping is AU4.

Medium info:
  Type:SDH, Line Coding:NRZ, Line Type:Short SM

Regenerator Section Status:
  No alarms detected.

Multiplex Section Status:
  No alarms detected.

Higher Order Path Status:
  Path# 1 has no defects

Lower Order Path Status:
  VC-12 1/1/1/1 has no defects
  VC-12 1/1/1/2 has no defects
  VC-12 1/1/1/3 has no defects
  VC-12 1/1/2/1 has no defects
[display text omitted]

Regenerator Section:
  INTERVAL       CV    ES   SES  SEFS
  20:47-20:50     0     0     0     0

Multiplex Section:
  INTERVAL       CV    ES   SES   UAS
  20:47-20:50     0     0     0     0

Higher Order Path:
  Path# 1:
```

```
  INTERVAL       CV    ES   SES   UAS
  20:47-20:50     0     0     0     0

Lower Order Path:
  AU-4# 1, TUG-3# 1, TUG-2# 1 VC-12# 1:
  INTERVAL       CV    ES   SES   UAS
  20:47-20:50     0     0     0     0

  AU-4# 1, TUG-3# 1, TUG-2# 1 VC-12# 2:
  INTERVAL       CV    ES   SES   UAS
  20:47-20:50     0     0     0     0

  AU-4# 1, TUG-3# 1, TUG-2# 1 VC-12# 3:
  INTERVAL       CV    ES   SES   UAS
  20:47-20:50     0     0     0     0
[display text omitted]

SONET 2/0/0   E1   1/1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  20:47-20:50     0     0     0     0     0     0     0     0     0     0     0
SONET 2/0/0   E1   1/1/1/2 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  20:47-20:50     0     0     0     0     0     0     0     0     0     0     0
SONET 2/0/0   E1   1/1/1/3 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  20:46-20:50     0     1     0     0     0     0     0     0     0    32     0
[display text omitted]
```

When AUG mapping is AU-3, view information about the SONET controller by using the **sonet controller sonet** *slot/port* [**brief** | **tabular**] command for a Cisco 7200 series router. Use the **sonet controller sonet** *slot/port-adapter/port* [**brief** | **tabular**] command for a Cisco 7500 series router.

The following examples show sample output for a Cisco 7500 series router:

```
Router# show controller sonet 2/0/0
SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
  Applique type is Channelized Sonet/SDH
  Clock Source is Internal, AUG mapping is AU3.

Medium info:
  Type:SDH, Line Coding:NRZ, Line Type:Short SM

Regenerator Section Status:
  No alarms detected.

Multiplex Section Status:
  No alarms detected.

Higher Order Path Status:
  Path# 1 has no defects
  Path# 2 has no defects
  Path# 3 has no defects

Lower Order Path Status:
  VC-12 1/1/1 has no defects
  VC-12 1/1/2 has no defects
  VC-12 1/1/3 has no defects
  VC-12 1/2/1 has no defects
[display text omitted]
Data in current interval (85 seconds elapsed):
   Regenerator Section:
     0 CVs, 0 ESs, 0 SESs, 0 SEFSs
   Multiplex Section:
     0 CVs, 0 ESs, 0 SESs, 0 UASs
   Higher Order Path:
     Path# 1: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     Path# 2: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     Path# 3: 0 CVs, 0 ESs, 0 SESs, 0 UASs
   Lower Order Path:
     VC-12 1/1/1: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     VC-12 1/1/2: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     VC-12 1/1/3: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     VC-12 1/2/1: 0 CVs, 0 ESs, 0 SESs, 0 UASs
     VC-12 1/2/2: 0 CVs, 0 ESs, 0 SESs, 0 UASs
[display text omitted]

SONET 2/0/0   E1   1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  Data in current interval (85 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
SONET 2/0/0   E1   1/1/2 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  Data in current interval (85 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
[display text omitted]

Router# show controller sonet 2/0/0 brief
SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
  Applique type is Channelized Sonet/SDH
  Clock Source is Internal, AUG mapping is AU3.

Medium info:
  Type:SDH, Line Coding:NRZ, Line Type:Short SM

Regenerator Section Status:
  No alarms detected.

Multiplex Section Status:
  No alarms detected.

Higher Order Path Status:
  Path# 1 has no defects
  Path# 2 has no defects
  Path# 3 has no defects

Lower Order Path Status:
  VC-12 1/1/1 has no defects
  VC-12 1/1/2 has no defects
  VC-12 1/1/3 has no defects
  VC-12 1/2/1 has no defects
[display text omitted]
SONET 2/0/0   E1   1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
SONET 2/0/0   E1   1/1/2 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
SONET 2/0/0   E1   1/1/3 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
[display text omitted]

Router# show controller sonet 2/0/0 tabular
SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
  Applique type is Channelized Sonet/SDH
  Clock Source is Internal, AUG mapping is AU3.

Medium info:
  Type:SDH, Line Coding:NRZ, Line Type:Short SM

Regenerator Section Status:
  No alarms detected.

Multiplex Section Status:
  No alarms detected.

Higher Order Path Status:
  Path# 1 has no defects
  Path# 2 has no defects
  Path# 3 has no defects

Lower Order Path Status:
  VC-12 1/1/1 has no defects
  VC-12 1/1/2 has no defects
  VC-12 1/1/3 has no defects
  VC-12 1/2/1 has no defects
[display text omitted]
Regenerator Section:
  INTERVAL       CV    ES   SES  SEFS
  21:22-21:24     0     0     0     0

Multiplex Section:
  INTERVAL       CV    ES   SES   UAS
  21:22-21:24     0     0     0     0

Higher Order Path:
  Path# 1:
  INTERVAL       CV    ES   SES   UAS
  21:22-21:24     0     0     0     0

  Path# 2:
  INTERVAL       CV    ES   SES   UAS
  21:22-21:24     0     0     0     0

  Path# 3:
  INTERVAL       CV    ES   SES   UAS
  21:22-21:24     0     0     0     0
```

```
Lower Order Path:
  AU-3# 1, TUG-2# 1 VC-12# 1:
  INTERVAL       CV    ES   SES   UAS
  21:22-21:24     0     0     0     0

  AU-3# 1, TUG-2# 1 VC-12# 2:
  INTERVAL       CV    ES   SES   UAS
  21:22-21:24     0     0     0     0

  AU-3# 1, TUG-2# 1 VC-12# 3:
  INTERVAL       CV    ES   SES   UAS
  21:22-21:24     0     0     0     0
[display text omitted]

SONET 2/0/0   E1   1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  21:22-21:24     0     0     0     0     0     0     0     0     0     0     0
SONET 2/0/0   E1   1/1/2 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  21:22-21:24     0     0     0     0     0     0     0     0     0     0     0
SONET 2/0/0   E1   1/1/3 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  21:22-21:24     0     0     0     0     0     0     0     0     0     0     0
[display text omitted]
```

When AUG mapping is AU-4, view information about a specific E1 line of a SONET controller by using the **show controller sonet** *slot/port.au-4-number/tug-3-number/tug-2-number/e1-number* [**brief** | **tabular**] command for a Cisco 7200 series router.

Use the **show controller sonet** *slot/port-adapter/port.au-4-number/tug-3-number/tug-2-number/e1-number* [**brief** | **tabular**] command for a Cisco 7500 series router. This command displays error and performance statistics.

The following examples show sample output for a Cisco 7500 series router:

```
Router# show controller sonet 2/0/0.1/1/1/1

SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
SONET 2/0/0   E1   1/1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  Data in current interval (237 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs

Router# show controller sonet 2/0/0.1/1/1/1 brief

SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
SONET 2/0/0   E1   1/1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.

Router# show controller sonet 2/0/0.1/1/1/1 tabular

SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
SONET 2/0/0   E1   1/1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  20:47-20:51     0     0     0     0     0     0     0     0     0     0     0

Router# show controller sonet 0/0/0.1/2/4/1 brief

SONET 0/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version : 0.2.3, ROM Version : 1.2
  FREEDM version : 2, F/W Version : 0.14.0
SONET 0/0/0   E1   1/2/4/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is line, National bits are 0x1F.


Router# show controller sonet 0/0/0.1/2/4/1 tabular

SONET 0/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version : 0.2.3, ROM Version : 1.2
  FREEDM version : 2, F/W Version : 0.14.0
SONET 0/0/0   E1   1/2/4/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is line, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  16:56-16:57     0     0     0     0     0     0     0     0     0     1     0
```

When AUG mapping is AU-3, view information about a specific E1 line of a SONET controller by using the **show controller sonet** *slot/port.au-3-number/tug-2-number/e1-number* [**brief** | **tabular**] command for a Cisco 7200 series router.

Use the **show controller sonet** *slot/port-adapter/port.au-3-number/tug-2-number/e1-number* [**brief** | **tabular**] command for a Cisco 7500 series router. This command displays error and performance statistics.

The following examples show sample output for a Cisco 7500 series router:

```
Router# show controller sonet 2/0/0.1/1/1

SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
SONET 2/0/0   E1   1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  Data in current interval (175 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
```

```
Router# show controller sonet 2/0/0.1/1/1 brief

SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version :0.2.3, ROM Version :1.2
  FREEDM version :2, F/W Version :1.2.0
SONET 2/0/0   E1   1/1/1 is up
  No alarms detected.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.

Router# show controller sonet 2/0/0.1/1/1 brief

SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version : 0.2.3, ROM Version : 1.2
  FREEDM version : 2, F/W Version : 0.14.0
SONET 2/0/0   E1   1/1/1 is down
  Transmitter is sending LOF Indication (RAI).
  Receiver has loss of frame.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.

Router# show controller sonet 2/0/0.1/1/1 tabular

SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version : 0.2.3, ROM Version : 1.2
  FREEDM version : 2, F/W Version : 0.14.0
SONET 2/0/0   E1   1/1/1 is down
  Transmitter is sending LOF Indication (RAI).
  Receiver has loss of frame.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  17:26-17:29     0     0     0     0     0     0     0     0     0   173     0
  17:11-17:26     0     0     0     0     0     0     0     0     0   471     0
  16:56-17:11     0     0     0     0     0     0     0     0     0     0     0
  16:41-16:56     0     0     0     0     0     0     0     0     0     0     0
  16:26-16:41     0     0     0     0     0     0     0     0     0   216     0
  16:11-16:26     0     0     0     0     0     0     0     0     0   225     0
  Total           0     0     0     0     0     0     0     0     0   912     0
```

Monitoring and Maintaining the PA-MC-STM-1

To monitor and maintain the PA-MC-STM-1, use the **show interface** command.

The following sample output displays the interface statistics of a PA-MC-STM-1 in port adapter slot 0 of a VIP4 in interface processor slot 2 of a Cisco 7500 series router:

```
Router# show interface serial 2/0/0.1.1.1.1:1

Serial2/0/0.1/1/1/1:1 is up, line protocol is up
Hardware is cyBus Channelized OC3/STM-1 PA
Internet address is 105.105.105.1/24
MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec, rely 255/255, load 36/255
Encapsulation HDLC, loopback not set
Keepalive not set
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations  0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 286000 bits/sec, 36 packets/sec
5 minute output rate 284000 bits/sec, 36 packets/sec
8019 packets input, 11695347 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
7991 packets output, 11650799 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
2 carrier transitions no alarm present
Timeslot(s) Used:1-31, Transmitter delay is 0 flags, transmit queue length 6
[Additional display text for remaining interfaces omitted]
```

Configuration Examples

This section provides the following configuration examples:

- Configuring the PA-MC-STM-1 Example
- Configuring a Logical Channel Group on an E1 Line Example
- Configuring a Channel Group Interface Example
- Configuring an E1 Unframed Channel Example

Configuring the PA-MC-STM-1 Example

You can configure each of the AUGs and TUGs of a PA-MC-STM-1 to carry a set of E1 links that are mapped into tributary unit level-12s (TU-12s).

In the following example, SDH framing, internal clock source, AUG mapping au-4 and idle pattern are configured:

```
Router(config)# controller sonet 1/0
Router(config-controller)# framing sdh
Router(config-controller)# clock source internal
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# mode c-12
Router(config-ctrlr-tug3)# tug-2 4 e1 channel-group 15 timeslots 1-5, 20-23
Router(config-ctrlr-tug3)# idle pattern 0x0
```

Configuring a Logical Channel Group on an E1 Line Example

To configure a logical channel group on an E1 line, use the **tug-2** *tug-2-number* **e1** *e1-number* **channel-group** *channel-group-number* **timeslots** *list-of-timeslots* command. In the following example, logical channel group 15 on E1 line 1 is configured and channelized time slots 1 to 5 and 20 to 23 are assigned to the newly created logical channel group:

```
Router(config)# controller sonet 1/0/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# mode c-12
Router(config-ctrlr-tug3)# tug-2 4 e1 1 channel-group 15 timeslots 1-5, 20-23
```

Configuring a Channel Group Interface Example

Once a channel group has been created, interface serial configuration commands may be used as in the following example:

```
Router(config)# controller sonet 1/0/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# mode c-12
Router(config-ctrlr-tug3)# tug-2 4 e1 10 channel-group 15 timeslots 1-5, 20-23
Router(config-ctrlr-tug3)# exit
Router(config-controller)# exit
Router(config)# interface serial 1/1/0.1/2/4/1:15
Router(config-if)# ip address 1.1.1.10 255.255.255.252
Router(config-if)# encapsulation ppp
```

Configuring an E1 Unframed Channel Example

To create an unframed or clear channel logical channel group on an E1 line, use the **tug-2** *tug-2-number* **e1** *e1-number* **unframed** command, as shown in the following example:

```
Router(config)# controller sonet 1/0/0
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 unframed
Router(config-ctrlr-tug3)# mode c-12
```

Command Reference

The following 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.

- **au-3**
- **au-4 tug-3**
- **aug mapping**
- **framing**
- **mode**
- **tug-2 e1 bert pattern**
- **tug-2 e1 channel-group timeslots**
- **tug-2 e1 clock source**
- **tug-2 e1 framing**
- **tug-2 e1 loopback**
- **tug-2 e1 national bits**
- **tug-2 e1 shutdown**
- **tug-2 e1 unframed**

Glossary

AUG—administrative unit group in SDH mode

BER—bit error rate

CAS—channel-associated signalling

CRC4—cyclic redundancy check. Error-checking technique in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending node.

E1—A digital carrier used to transmit a formatted signal at 2.048 Mbps.

ITU—International Telecommunication Union–Telecommunication standards sector

PRI—Primary Rate Interface

SDH—synchronous digital hierarchy. The ITU equivalent of SONET.

SONET—Synchronous Optical Network. The ANSI specification describing the data format used in high-speed optical data transmission

STM-n—Synchronous Transport Module level-n (STM-1 is 155.52 Mbps.)

TU-n—tributary unit level-n

TUG-n—tributary unit group-n

VC—virtual circuit

VC-n—virtual container level-n

VIP—Virtual Interface Processor

PA-MC-2T3+ Phase-II (T3 subrate)

Feature History

Release	Modification
12.1(5a)E	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This feature module describes the availability of clear channel (T3 subrate) on the two-port enhanced multichannel T3 port adapter (PA-MC-2T3+). It includes information on the benefits of this new feature, supported platforms, configuration examples, and a command reference.

This document contains the following sections:

Feature Overview

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections. Each T3 interface can now be independently configured to be either channelized or unchannelized. A channelized T3 provides 28 T1 lines multiplexed into the T3. Each T1 line can be configured into one or more serial interface data channels.

Using the **no channelized** command, you can configure the T3 as a single, unchannelized serial interface data channel. You can configure this data channel to use all of the T3 bandwidth or a portion of it.

Benefits

The PA-MC-2T3+ now provides the following benefits:

- Two T3 ports each with integrated CSU/DSUs
- Two T3 ports on one single-wide port adapter
- Up to 256 logical, T1 n x 56K and n x 64K channels
- 28 T1 ports multiplexed into a single T3 connection
- Channelized T1, fractional T1, and full-rate T1 support
- Subrate and full rate T3 support
- Line and payload loopback capabilities
- Full bit error rate testing on any T1 or any unchannelized T3
- DSX-3 level interface
- Full duplex and connectivity at DS3 rate (44.736 Mbps)
- T3 Scrambling and subrate can be independently or simultaneously enabled in each DSU mode
- C-bit or M13 framing
- B3ZS line coding
- DS3 FEAC channel support
- Support for Frame Relay, PPP, HDLC, SMDS DXI, and X.25

Restrictions

The PA-MC-2T3+ does not support the following:

- More than 128 channels per T3
- Use of unused channels of one T3 by the other T3

Related Features and Technologies

- PA-MC-T3
- PA-2T3+
- PA-MC-2T3+ Phase I

Related Documents

PA-MC-2T3+ Multi-Channel T3 Port Adapter Installation and Configuration

Supported Platforms

- Cisco 7200 series
- Cisco 7500 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 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

- ANSI T1.102
- ANSI T1.107
- ANSI T1.403
- ANSI T1.404
- AT&T 62411
- AT&T 54016
- AT&T 54014
- AT&T TR-NWO-00499
- FCC Part 68
- FCC Part 15, Class A
- UL1950 3rd Edition/CSA C22.2, No. 950

MIBs

No new or modified 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://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

- RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types*
- RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type*

Configuration Tasks

See the following sections for configuration tasks for the T3 subrate feature. Each task in the list is identified as either required or optional.

- Configuring the T3 Controller (required)
- Configuring the Serial Interface (required)
- Verifying the Configuration (optional)

Configuring the T3 Controller

	Command	Purpose
Step 1	Cisco 7200 series routers Router(config)# **controller T3** *chassis-slot/T3-port* Cisco 7500 series routers Router(config)# **controller T3** *interface-processor-slot/port-adapter-slot/T3-port*	Select the T3 controller you want to configure.
Step 2	Router(config-controller)# **no channelized** Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]: **Y**	Configures unchannelized mode for the T3 controller. When the PA-MC-2T3+ is configured for unchannelized T3 mode, the default MTU size is set to 4470 for compatibility with other T3 equipment and port adapters. The change in MTU sizes will cause a memory recarve and CBus complex to occur, disrupting all traffic on the router for several minutes. (This occurs only on Cisco 7500 series routers.) Type Y for “yes” at the end of the warning. At the prompt, type **^Z** to exit. You will exit configuration mode, and enter unchannelized mode.

	Command	Purpose
Step 3	`Router(config-controller)# bert pattern pattern interval time`	Sends a BERT pattern on the T3 line to test cable and signal problems in the field. - *pattern*: – **0s**, repetitive test pattern of all zeros (00000) – **1s**, repetitive test pattern of all ones (11111) – **2^15**, pseudorandom 0.151 test pattern (32,768 bits long) – **2^20**, pseudorandom 0.151 test pattern (1,046,575 bits long) – **2^23**, pseudorandom 0.151 test pattern (8,388,607 bits long) – **alt-0-1**, repetitive alternating test pattern of zeros (0s) and ones (1s), (01010101) - *time*—1–14400 minutes

	Command	Purpose
Step 4	Router(config-controller)# **mdl** {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} **string**}	Configures Maintenance Data Link (MDL) messages on the PA-MC-2T3+. **Note** MDL messages are only supported when the T3 framing is set for C-bit. • **transmit path**—Enables transmission of the MDL path message • **transmit idle-signal**—Enables transmission of the MDL idle-signal message • **eic—**Equipment identification code (up to 10 characters) • **lic**—Location identification code (up to 11 characters) • **fic**—Frame identification code (up to 10 characters) • **unit**—Unit identification code (up to 6 characters) • **pfi**—Facility identification code to send in the MDL path message (up to 38 characters) • **port**—Equipment port, which initiates the idle signal, to send in the MDL idle signal message (up to 38 characters) • **generator**—Generator number to send in the MDL test signal message (up to 38 characters) Use the **no** form of this command to remove MDL messages. The default is that no MDL message is configured.

Configuring the Serial Interface

	Command	Purpose

Step 1	Cisco 7200 series routers:
	`Router# configuration terminal`
	`Router(config)# controller T3 chassis-slot/T3-port`
	or
	Cisco 7500 series routers:
	`Router# configuration terminal`
	`Router(config)# interface serial interface-processor-slot/port-adapter-slot/T3-port`
		Enables interface configuration mode and selects a serial interface to configure.

Step 2	`Router(config-if)# framing {c-bit | m13}`	Specifies the T3 framing on the serial interface. • **c-bit**—C-bit parity DS3 framing • **m13**—M13 Multiplex DS3 framing The default is C-bit framing.
Step 3	`Router(config-if)# cablelength feet`	Specifies the cable length. • *feet*—A numeral from 0 to 450
Step 4	`Router(config-if)# clock source {line | internal}`	Sets the clock source for the selected T3 interface. • **line**—Selects a network clock source • **internal**—Selects an internal clock source
Step 5	`Router(config-if)# dsu mode [ 0 | 1 |2 | 3 | 4 ]`	Configures the PA-MC-2T3+ to emulate a proprietary DSU subrate scheme. • **0**—Digital Link or Cisco—300-44210 Kbps • **1**—ADC Kentrox T3/E3 IDSU—1500-35000, 44210 Kbps • **2**—Larscom Access T45—3100-44210 Kbps • **3**—Adtran T3SU 300—75-44210 Kbps • **4**—Verilink HDM 2182—1500-44210 Kbps Default is **0**.
Step 6	`Router(config-if)# dsu bandwidth bandwidth`	Configures the bandwidth for an unchannelized subrate T3 interface. • *bandwidth*—A Numeric value between 1 and 44210 The default bandwidth is 44210.

Verifying the Configuration

After configuring a new T3 controller, you can verify the configuration by using **show** commands. To display the status of any a new T3 controller or newly configured interface, complete any of the following tasks in EXEC mode:

Step 1 Display the status of the T3 controller on a Cisco 7200 series router using the **show controllers t3** *port-adapter/t3-port* [**brief | tabular**] command.

or

Display the status of the T3 controller on a Cisco 7500 series router using the **show controllers t3** *slot/port-adapter/t3-port* [**brief | tabular**] command:

```
Router# show controllers t3 0/1/0 brief
T3 0/1/0 is up.  Hardware is 2CT3+ single wide port adapter
  CT3 H/W Version: 0.1.1, CT3 ROM Version: 0.95, CT3 F/W Version: 2.4.0
  FREEDM version: 1, reset 0
  Applique type is Subrate T3
  No alarms detected.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Line
  Rx throttle total 0, equipment customer loopback


Router# show controllers t3 0/1/0 tabular
T3 0/1/0 is up.  Hardware is 2CT3+ single wide port adapter
  CT3 H/W Version: 0.1.1, CT3 ROM Version: 0.95, CT3 F/W Version: 2.4.0
  FREEDM version: 1, reset 0
  Applique type is Subrate T3
  No alarms detected.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Line
  Rx throttle total 0, equipment customer loopback
  INTERVAL      LCV   PCV   CCV   PES  PSES  SEFS   UAS   LES   CES  CSES
  06:17-06:24     0     0     0     0     0     1     0     0     0     0
  06:02-06:17     4     2     1     1     0     0     1     0     0     0
  05:47-06:02     0     0     0     0     0     0     0     0     0     0
  05:32-05:47     0     0     0     0     0     0     0     0     0     0
  05:17-05:32     0     0     0     0     0     0     0     0     0     0
  05:02-05:17     0     0     0     0     0     0     0     0     0     0
  04:47-05:02     0     0     0     0     0     0     0     0     0     0
  04:32-04:47     0     0     0     0     0     0     0     0     0     0
  04:17-04:32     0     0     0     0     0     0     0     0     0     0
  04:02-04:17     0     0     0     0     0     0     0     0     0     0
  03:47-04:02     0     0     0     0     0     0     0     0     0     0
  03:32-03:47     0     0     0     0     0     0     0     0     0     0
  03:17-03:32     0     0     0     0     0     0     0     0     0     0
[additional command output omitted]
```

Use the **show interfaces serial** *port-adapter/t3-port* command to display statistics about the serial interface for a specific T3 line on a Cisco 7200 series router:

```
Router# show interfaces serial 5/0
Serial5/0 is up, line protocol is down
  Hardware is PA-MC-2T3+
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
    reliability 128/255, txload 1/255, rxload 1/255
 Encapsulation HDLC, crc 16, loopback not set
 Keepalive set (10 sec)
 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 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5823 packets output, 140669 bytes, 0 underruns
    0 output errors, 0 applique, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions
DSU mode 0, bandwidth 44210, scramble 0
```

or
Display statistics about the serial interface for a specific T3 line on a Cisco 7500 series router using the **show interfaces serial** *slot/port-adapter/t3-port* command:

```
Router# show interfaces serial 1/0/0
Serial1/0/0 is up, line protocol is up
  Hardware is cyBus 2CT3+ Serial
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:09, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 4 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
     4 packets input, 402 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
              0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 1 abort
     5 packets output, 1008 bytes, 0 underruns
     0 output errors, 0 applique, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
 DSU mode 0, bandwidth 44210, scramble 0
```

Troubleshooting Tips

Set loopbacks to troubleshoot the PA-MC-2T3+.

Setting Loopbacks

You can configure the T3 controller for loopback modes using the serial interface **loopback** command. The default is no loopback. The three main loopback modes are: local, network, and remote. The T3 local loopback simultaneously loops the T3 port toward the router and loops the T3 link back toward the network.

The T3 network loopback loops the T3 line or payload back toward the network. A T3 remote loopback loops the T3 line at the remote end. Use T3 loopbacks to diagnose problems with cables between the port adapter and the central switching office at the T3 line level. You can also use the loopback modes with bit error rate (BER) tests.

To set a loopback on the T3 controller or T3 lines, perform the following optional tasks beginning in global configuration mode:

	Command	Task

Step 1	`Router(config)# interface serial slot/port-adapter/port`
	(Cisco 7500 series and Cisco 7000 series routers with RSP)
	`Router(config)# interface serial slot/port`
	(Cisco 7200 series)
		Select the T3 serial interface and enter interface configuration mode.

Step 2	`Router(config-controller)# loopback {local | network | remote}`	Set a loopback on the T3 controller.

Monitoring and Maintaining the PA-MC-2T3+

Command	Purpose

Cisco 7200 series routers:
`Router# show controllers T3 slot/t3-port`
Cisco 7500 series routers:
`Router# show controllers T3 slot/port-adapter/t3-port`
	Displays the configuration, including the results of BER tests, for a specified T3 controller.

Cisco 7200 series routers:
`Router# show interface serial slot/t3-port`
Cisco 7500 series routers:
`Router# show interface serial slot/port-adapter/t3-port`
	Displays the interface configuration of a specified serial interface.

Configuration Examples

This section provides the following configuration examples:

- Configuring a T3 Controller Example
- Configuring a Full-Rate T3 Interface Example
- Configuring a Subrate T3 Interface Example

Configuring a T3 Controller Example

The following example configures the T3 controller of a PA-MC-2T3+ in slot 1 of a Cisco 7200 series router:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# controller T3 1/0
Router(config-controller)# no channelized
Router(config-controller)# exit
Router(config)# interface serial 1/0/0
Router(config-if)# framing c-bit
Router(config-if)# cablelength 40
Router(config-if)# clock source line
Router(config-if)# mdl transmit path
```

The following example configures the T3 controller of a PA-MC-2T3+ on a VIP2 or VIP4 in interface processor slot 1 on a Cisco 7500 series router:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# controller T3 1/0/0
Router(config-controller)# no channelized

Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]:Y
Router(config-controller)# exit
Router(config)# interface serial 1/0/0
Router(config-if)# framing c-bit
Router(config-if)# cablelength 40
Router(config-if)# clock source line
Router(config-if)# mdl transmit path
```

Configuring a Full-Rate T3 Interface Example

The following example configures a full-rate T3 interface on a Cisco 7500 series router by using the **no channelized** command:

```
Router(config)# controller t3 2/0/0
Router(config-controller)# no channelized
Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]: Y
Router(config-controller)# exit
Router(config)# interface serial 2/0/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip address 10.10.10.10 255.255.255.255
Router(config-if)# no shutdown
```

Configuring a Subrate T3 Interface Example

In order to configure a subrate T3 interface, you must first configure the interface as a full-rate T3 using the **no channelized** configuration controller command. After the full-rate T3 interface is configured, use the **dsu bandwidth** command to create a subrate T3 interface.The following example configures a subrate T3 interface on a Cisco 7200 series router:

```
Router(config)# controller t3 2/0
Router(config-controller# no channelized
Router(config-controller)# exit
Router(config)# interface serial 2/0
Router(config-if)# dsu bandwidth 16000
Router(config-if)# encapsulation frame-relay
Router(config-if)# ip address 10.10.10.10 255.255.255.255
Router(config-if)# no shutdown
```

Command Reference

The following 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.

- **no channelized**

1/2 Port Channelized T1/E1 PRI Network Module (NM-1CE1T1-PRI and NM-2CE1T1-PRI)

The NM-1CE1T1-PRI (1-port) and NM-2CE1T1-PRI (2-port) network modules provide support for T1, E1, and ISDN primary rate interface (PRI) network connections in a network module form factor. This feature (referred to in this document as NM-xCE1T1-PRI) offers attachment of one T1, E1, or ISDN PRI line on the 1-port module and two T1, E1, or ISDN PRI lines on the 2-port version.

This new feature (NM-xCE1T1-PRI) enables you to configure a single network module as either a T1 interface or an E1 interface on the same card. The configuration of a T1 or E1 interface and the change from one to the other is controlled by the **card type** command. Additionally, when in E1 mode, the module can be configured between channelized E1, ISDN PRI, E1-CAS-R2, balanced and unbalanced, and structured (G.704) versus unstructured (G.703) modes. In T1 mode, the module can be configured for channelized T1, T1-CAS, and as a CSU/DSU.

Note After you insert the NM-xCE1T1-PRI feature network module into the router chassis, you *must* use the **card type** command in the command-line interface (CLI) to configure the NM-xCE1T1-PRI feature. The controller will not be detected and cannot be configured until you use the **card type** command.

Configuration of the T1 or E1 interface can be customized using command-line interface (CLI) commands. In E1 mode, each port can be individually set to 120-ohm or 75-ohm termination. Each port has RJ-48C connectors, and there is one bantam jack that is shared by each port (for 2-port cards) for monitoring.

Feature Specifications for the 1/2 Port Channelized T1/E1 PRI Network Module

Feature History	
Release	**Modification**
12.3(1)	This feature was introduced in Cisco IOS Release 12.3(1).
Supported Platforms	
Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745. This feature is not supported on the Cisco 3620 and Cisco 3640 platforms. For the Cisco 2600 series, only the Cisco 2610-2651XM series and Cisco 2691 are supported. Cisco 2610-2651 (non-XM) are not supported.	

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

Information About NM-xCE1T1-PRI Support

After you insert the NM-xCE1T1-PRI feature network module into the router chassis, you must use the **card type** command in the command-line interface (CLI) to configure the NM-xCE1T1-PRI feature. The controller will not be detected and cannot be configured until you use the **card type** command.

If the **card type** command is used to make subsequent changes, these changes will take effect only if you use the **reload** command after changing the card type.

The bantam jack can be connected only to one port at a time.

The NM-xCE1T1-PRI feature will not support channel service unit (CSU) DTE loopback or CSU network loopback modes. Because the CSU is integrated into the framer, there is no need or way to support CSU loopbacks.

To configure the NM-xCE1T1-PRI feature, you need to understand the following concepts:

- NM-xCE1T1-PRI Feature Driver Software, page 492
- NM-xCE1T1-PRI Feature Supported Functions, page 492

NM-xCE1T1-PRI Feature Driver Software

The driver software for the NM-xCE1T1-PRI feature provides for the transmission and reception of packets over channelized E1 and T1 circuits. Driver functions are as follows:

- Network Management Interface (MIB support)
- New CLI for 75-ohm and 120-ohm line termination for E1
- New CLI for specifying the card type (T1/E1)

NM-xCE1T1-PRI Feature Supported Functions

This section summarizes the functions supported by the NM-xCE1T11PRI feature.

- Two card versions:
  - 1-port T1 (DSU/CSU), E1 and G.703 (balanced and unbalanced)
  - 2-port T1 (DSU/CSU), E1 and G.703 (balanced and unbalanced)
- Four LEDs per port defined as Carrier Detect, Remote Alarm, Local Alarm, and Loopback
- Three LEDs per port defined as T1-100, E1-120, and E1-75
- RJ-48 connectors with transition cable breakout to physical media type
- T1 CSU and DSU line buildouts, E1 short haul and long haul
- T1 SF and ESF framing
- ANSI T1.403 Annex B/V.54 loopup/loopdown code recognition, network loopback, and user-initiated loopbacks
- E1 structured (ITU G.704) and unstructured (ITU G.703) operation
- AMI, B8ZS, and HDB3 line coding
- Two bantam jacks for TX and RX monitor with two LEDs defined as P0, P1 (port selected)

How to Configure the NM-xCE1T1-PRI Feature

This section describes the commands used to configure the NM-xCE1T1-PRI feature:

- Configuring an NM-xCE1T1-PRI Card for a T1 Interface, page 493
- Configuring an NM-xCE1T1-PRI Card for an E1 Interface, page 495
- Configuring a T1 or E1 Interface for Bantam-Jack Monitoring, page 497
- Verifying NM-xCE1T1-PRI Support, page 499

Configuring an NM-xCE1T1-PRI Card for a T1 Interface

Perform this task to select and configure a network module card as T1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **card type t1** *slot*
4. **controller t1** *slot*/*port*
5. **linecode** {**ami** | **b8zs**}
6. **framing** {**sf** | **esf**}
7. **clock source** {**line** | **internal**}
8. **pri-group** [**timeslots** *range*]
9. **exit**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`card type t1`** *`slot`*
	Example:
	`Router(config)# card type t1 1`
		Sets or changes the card type.
		• When the command is used for the first time, the configuration takes effect immediately.
		• A subsequent change in the card type will not take effect unless you enter the **reload** command or reboot the router.

Step 4	**`controller t1`** *`slot`*/*`port`*
	Example:
	`Router(config)# controller t1 1/0`
		Enters controller configuration mode and identifies the controller type (T1) and a slot and port for configuration commands that specifically apply to the T1 interface.
		• The **card type** command must be entered before this command can be used.

Step 5	**`linecode`** {**`ami`** | **`b8zs`**}
	Example:
	`Router(config-controller)# linecode b8zs`
		Specifies a line encoding for a controller.
		• The **controller** command must be entered before this command can be used.
		• Line-code value for T1 can be **ami** or **b8zs**.

Step 6	**`framing`** {**`sf`** | **`esf`**}
	Example:
	`Router(config-controller)# framing esf`
		Specifies a frame type.
		• The **controller** command must be entered before this command can be used.
		• The frame type can be specified as **sf** for superframe or **esf** for extended superframe for T1 controllers.

Step 7	**`clock source`** {**`line`** | **`internal`**}
	Example:
	`Router(config-controller)# clock source line`
		Sets the clock source for a T1 controller.
		• The clocking argument can have a value of **line** or **internal**.
		– A value of **line** means the source is the loop.
		– A value of **internal** means the source is the local oscillator if the card is not participating in the backplane timing domain.

	Command or Action	Purpose
Step 8	**pri-group** [**timeslots** *range*] **Example:** `Router(config-controller)# pri-group timeslots 1-5`	Specifies that the controller should be set up as a PRI interface. • For T1, the last defined channel is the D channel. • If a controller is configured as PRI, individual channel groups cannot be configured on that controller. • The **controller** command must be entered before this command can be used. **Note** To specify that the controller should be set up as a channel group, use the **channel-group** command here instead of the **pri-group** command. For more information, see the "Configuring an NM-xCE1T1-PRI Card for an E1 Interface" section on page 495.
Step 9	**exit** **Example:** `Router# exit`	Exits the controller configuration mode and returns the router to privileged EXEC mode.
Step 10	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the new configuration parameters to the permanent configuration file. • This command can be abbreviated to **copy run start**.

Configuring an NM-xCE1T1-PRI Card for an E1 Interface

Perform this task to select and configure an NM-xCE1T1-PRI network module card as E1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **card type e1** *slot*
4. **controller e1** *slot*/*port*
5. **linecode** {**ami** | **hdb3**}
6. **framing** {**crc4** | **no-crc4**}
7. **clock source** {**line** | **internal**}
8. **channel-group** *channel-number* {**timeslots** *range* [**speed** {**56** | **64**}] | **unframed**}
9. **line termination {75-ohm | 120-ohm}**
10. **exit**
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**card type e1** *slot* **Example:** `Router(config)# card type e1 1`	Sets or changes the card type. • When the command is used for the first time, the configuration takes effect immediately. • A subsequent change in the card type will not take effect unless you enter the **reload** command or reboot the router.
Step 4	**controller e1** *slot***/***port* **Example:** `Router(config)# controller e1 1/0`	Enters controller configuration mode and identifies the controller type (E1) and a slot and port for configuration commands that specifically apply to the E1 interface. • The **card type** command must be entered before this command can be used.

Step 5	**linecode** {**ami** | **hdb3**}
	Example:
	`Router(config-controller)# linecode hdb3`
		Specifies a line encoding for a controller.
		• The **controller** command must be entered before this command can be used.
		• Linecode value for E1 can be **ami** or **hdb3**.

Step 6	**framing** {**crc4** | **no-crc4**}
	Example:
	`Router(config-controller)# framing crc4`
		Selects a frame type.
		• The **controller** command must be entered before this command.
		• The framing value can be **crc4** or **no crc4** for E1 controllers.

Step 7	**clock source** {**line** | **internal**}
	Example:
	`Router(config-controller)# clock source line`
		Sets the clock source for an E1 controller.
		• The clocking argument can have a value of **line** or **internal**.
		– A value of **line** means the source is the loop.
		– A value of **internal** means the source is the local oscillator if the card is not participating in the backplane timing domain.

	Command or Action	Purpose

Step 8	**channel-group** *channel-number* {**timeslots** *range* [**speed** {**56** | **64**}] | **unframed**}
	Example:
	`Router(config-controller)# channel-group 1 unframed`
		Specifies that the controller should be set up as a channelized interface.
		• Defines the time slots that belong to each E1 circuit.
		• When a T1 data line is configured, channel-group numbers can be values from 0 to 23.
		• When an E1 data line is configured, channel-group numbers can be values from 0 to 30.
		• The **unframed** keyword specifies that all 32 time slots are used for data. None of the 32 time slots are used for framing signals.
		• The **controller** command must be entered before this command can be used.
		Note T o specify that the controller should be set up as a PRI group, use the **pri-group** command here instead of the **channel-group** command. For more information, see the "Configuring an NM-xCE1T1-PRI Card for a T1 Interface" section on page 493.

Step 9	**line-termination** {**75-ohm** | **120-ohm**}
	Example:
	`Router(config-controller)# line-termination 120-ohm`
		Configures the E1 line interface for 120-ohm or 75-ohm termination.
		• The **controller** command must be entered before this command can be used.
		• Line termination is configurable only for E1.

Step 10	**exit** **Example:** `Router# exit`	Exits the controller configuration mode and returns the router to privileged EXEC mode.
Step 11	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the new configuration parameters to the permanent configuration file. • This command can be abbreviated to **copy run start**.

Configuring a T1 or E1 Interface for Bantam-Jack Monitoring

Perform this task to enable monitoring of the TX and RX lines of a T1 or E1 port on the onboard bantam jack.

Note Only one port can be monitored at a time. Disable the bantam-jack monitoring if you are not *actively* monitoring the TX and RX activity for a port.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **card type** {**t1** | **e1**} *slot*
4. **controller** {**t1** | **e1**} *slot/port*
5. **bantam-jack enable**
6. **no bantam-jack enable**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`card type`** `{`**`t1`** `|` **`e1`**`}` *`slot`*
	Example:
	`Router(config)# card type e1 1`
		Sets or changes the card type.
		• When the command is used for the first time, the configuration takes effect immediately.
		• A subsequent change in the card type will not take effect unless you enter the **reload** command or reboot the router.

Step 4	**`controller`** `{`**`t1`** `|` **`e1`**`}` *`slot/port`*
	Example:
	`Router(config)# controller e1 1/0`
		Enters controller configuration mode and identifies the controller type (T1 or E1) and a slot and port for configuration commands that specifically apply to the T1 or E1 interface.
		• The **card type** command must be entered before this command can be used.

Step 5	**`bantam-jack enable`**
	Example:
	`Router(config-controller)# bantam-jack enable`
		Monitors the TX and RX lines of a T1 or E1 port on the onboard bantam jack.
		• Only one port can be monitored at a time.

	Command or Action	Purpose
Step 6	**no bantam-jack enable** **Example:** `Router(config-controller)# no bantam-jack enable`	Disables the monitoring function of the TX and RX lines of a T1 or E1 port on the onboard bantam jack. • Only one port can be monitored at a time. • Always disable the monitoring function of the TX and RX lines when you are not actively monitoring the lines.
Step 7	**exit** **Example:** `Router# exit`	Exits controller configuration mode and returns the router to privileged EXEC mode.

Verifying NM-xCE1T1-PRI Support

To examine the state of the T1 or E1 line, use the **show controller** and **show interface** commands.

SUMMARY STEPS

1. **enable**
2. **show controller** {**t1** | **e1**}
3. **show interfaces serial** *slot***/***port***:**[*channel-group*]
4. **show pci bridge** *slot-number*

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

Step 2	**show controller** {**t1** | **e1**}
	Example:
	`Router# show controller t1`
		Displays the RFC 1406 MIB statistics about the T1 or E1 port, card revision information, alarm status, and port configuration.

	Command or Action	Purpose
Step 3	**show interfaces serial** *slot***/***port*:[*channel-group*] **Example:** `Router# show interfaces serial 1/0:23`	Displays statistics for channels and channel groups created within a T1 or E1 controller, which are treated as serial interfaces. • The range of slot numbers is dependent on the host router. • The port can be either 0 or 1. • Channel-group values range from 0 to 23 for T1 controllers and from 0 to 30 for E1 controllers. • The channel group is the number parameter defined in the **channel-group** command. • If no *channel-group* value is entered, all the interfaces are displayed.
Step 4	**show pci bridge** *slot-number* **Example:** `Router# show pci bridge 1`	Displays peripheral component interconnect (PCI) configuration information about the port module in a particular slot, including any bridges on both the host router and the network module.

Examples

This section describes commands that can be used to examine the state of the T1 or E1 lines.

- Using the show controller Command Example, page 500
- Using the show interfaces Command Example, page 501
- Using the show interfaces Command for a Particular Slot or Port Example, page 501

Using the show controller Command Example

The following is example output from a **show controller** command:

```
Router#show controller E1
E1 1/0 is up.
  Applique type is Channelized E1 - balanced
  No alarms detected.
  alarm-trigger is not set
  Framing is UNFRAMED, Line Code is HDB3, Clock Source is Line.
  Bantam Jack Enabled                  <---- indicates bantam-jack monitoring is enabled
  Module type is Channelized E1/T1 PRI
  Version info Firmware: 0000001D, FPGA: 0
  Hardware revision is 0.2          , Software revision is 29
  Protocol revision is 1
  number of CLI resets is 1
  Last clearing of alarm counters 00:00:10
    receive remote alarm  :    0,
    transmit remote alarm :    0,
    receive AIS alarm     :    0,
    transmit AIS alarm    :    0,
    loss of frame         :    0,
    loss of signal        :    0,
    Loopback test         :    0,
    transmit AIS in TS 16 :    0,
    receive LOMF alarm    :    0,
    transmit LOMF alarm   :    0,
  MIB data updated every 10 seconds.
  Data in current interval (10 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Using the show interfaces Command Example

The following is example output from a **show interfaces** command:

```
Router# show interfaces serial 0/0:0

Serial0/0:0 is up, line protocol is up
Hardware is DSX1
Internet address is 10.0.0.1 255.0.0.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 9/255
Encapsulation HDLC, loopback not set, keepalive not set
Last input 0:15:34, output 0:00:00, output hang never
Last clearing of "show interface" counters never
Output queue 2/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 56000 bits/sec, 195 packets/sec
5 minute output rate 56000 bits/sec, 196 packets/sec
8728809 packets input, 338385740 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    8729371 packets output, 338413798 bytes, 0 underruns
    0 output errors, 0 collisions, 6 interface resets, 0 restarts
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
.
.
.
Serial0/0:23 is up, line protocol is up
Hardware is DSX1
Internet address is 10.0.0.2 255.0.0.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 9/255
Encapsulation HDLC, loopback not set, keepalive not set
Last input 0:15:34, output 0:00:00, output hang never
Last clearing of "show interface" counters never
Output queue 2/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 56000 bits/sec, 195 packets/sec
5 minute output rate 56000 bits/sec, 196 packets/sec
8728809 packets input, 338385740 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    8729371 packets output, 338413798 bytes, 0 underruns
    0 output errors, 0 collisions, 6 interface resets, 0 restarts
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Using the show interfaces Command for a Particular Slot or Port Example

The following is example output from a **show interfaces** command for a particular slot or port:

```
Router# show interfaces serial 1/0:18

Serial 1/0:18 is up, line protocol is up
Hardware is DSX1
Internet address is 10.0.0.2 255.0.0.0
MTU 1500 bytes, BW 9 Kbit, DLY 100000 usec, rely 255/255, load 1/255
```

```
Encapsulation SLIP, loopback not set
DTR is pulsed for 5 seconds on reset
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Output queue 0/10, 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 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
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The commands to display the accounting and statistics on a particular interface will be the **show interfaces** *interface* **1/0:18 accounting** and **show interface** *interface* **1/0:18 stats** commands. The output for these cases will be identical to that for all other Cisco interfaces.

Configuration Examples for NM-xCE1T1-PRI Support

This section shows example configuration files for a T1 interface and an E1 interface.

- T1 Interface Example, page 502
- E1 Interface Example, page 504

T1 Interface Example

This sample configuration is for a Cisco 3745 with two cards in slots 1 and 3 configured for T1:

```
Router# show running configuration

Building configuration...

Current configuration: 1744 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host1
!
card type t1 1
card type t1 3
!
ip subnet-zero
!
!
!
isdn switch-type primary-dms100
!
!
voice call carrier capacity active
!
!
!
!
```

```
!
!
!
!
!
mta receive maximum-recipients 0
!
controller T1 1/0
 framing esf
 linecode b8zs
 cablelength long 0db
 pri-group timeslots 1-24
!
controller T1 1/1
 framing esf
 linecode b8zs
 cablelength long 0db
 pri-group timeslots 1-24
!
controller T1 3/0
 framing esf
 linecode b8zs
 cablelength long 0db
 pri-group timeslots 1-24
!
controller T1 3/1
 framing esf
 linecode b8zs
 cablelength long 0db
 pri-group timeslots 1-24
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 speed 100
 full-duplex
!
interface Serial0/0
 no ip address
 clockrate 2000000
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed 10
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial1/0:23
 no ip address
 isdn switch-type primary-dms100
 no cdp enable
!
interface Serial1/1:23
 no ip address
 isdn switch-type primary-dms100
 no cdp enable
!
interface FastEthernet2/0
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface TokenRing2/0
 no ip address
 shutdown
 ring-speed 16
!
interface Serial3/0:23
 no ip address
 isdn switch-type primary-dms100
 no cdp enable
!
interface Serial3/1:23
 no ip address
 isdn switch-type primary-dms100
 no cdp enable
!
ip classless
ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

E1 Interface Example

```
Current configuration : 1667 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
card type e1 1
no logging buffered
!
```

```
ip subnet-zero
!
!
isdn switch-type primary-net5
!
!
!
controller E1 1/0
 channel-group 1 unframed
!
controller E1 1/1
 channel-group 1 unframed
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 load-interval 30
 shutdown
 speed 100
 full-duplex
 no cdp enable
!
interface 1/0:1
 no ip address
!
interface 1/1:1
 no ip address
!
!
ip http server
ip classless
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 login
!
!
end
```

Additional References

The following sections provide additional references related to the NM-xCE1T1-PRI feature:

- Related Documents, page 506
- Standards, page 506
- MIBs, page 506
- RFCs, page 506
- Technical Assistance, page 506

Related Documents

Related Topic	Document Title
Hardware installation instructions for the 1/2 Port Channelized T1/E1 PRI Network Module	*Cisco Network Module Hardware Installation Guide*

Standards

Standards	Title
ANSI T1.403-1995	*Network to Customer Installation—DS1 Metallic Interface*
ITU Recommendation G.703	*Physical/Electrical Characteristics of Hierarchical Digital Interfaces* (July 1988)
AT&T Publication 54016	*Requirements for Interfacing Digital Terminal Equipment to Services Employing the Extended Super Frame Format*

MIBs

MIBs	MIBs Link
• CISCO-ICSUDSU-MIB • RFC 1406 MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1406	*Definitions of Managed Objects for the DS1 and E1 Interface Types*

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, tools, and lots more. 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.

- **bantam-jack enable**
- **card type**
- **channel-group**
- **controller**
- **pri-group**

Glossary

AIS—T1 alarm indication signal.

AMI—alternate mark inversion. A bipolar return to zero line encoding scheme.

ANSI T1.403-1995—Network to Customer Installation—DS1 Metallic Interface.

ATM—Asynchronous Transfer Mode.

BERT—bit error rate tester.

BPV—bipolar violation (AMI) same polarity as previous pulse.

CAS—channel-associated signaling.

CCC—clear channel capability (64 kbps data channels for DS1).

CRC—cyclic redundancy check.

CSM—call switching module.

CSU—channel service unit.

DSP—digital signal processor.

DSU—data service unit.

E1—European equivalent of T1, 32 channels of 64 kHz each, 1 for framing, 1 for signaling.

ESF—extended super frame, 24 frames per ESF, includes additional signaling.

FAS—frame align signal.

FDL—facilities data link.

FPGA—field programmable gate array.

HDB3—high density binary 3 zero suppression.

HDLC—High-Level Data Link Control protocol.

LCV—line code violation—occurrence of BPV.

LIU—line interface unit.

LOS—loss of signal.

MARS—modular access routers.

MIB—Management Information Base.

OOF—out of frame (G.706) Consecutive frame alignment signals received in error.

PCI—peripheral component interconnect. Specification that defines the PCI local bus.

PCV—path code violation—(unframed) frame sync bit error, (framed) CRC.

PRI—Primary Rate Interface.

SES—severely errored second.

SF—Super frame, or D4 framing, 12 frames per super frame for in-band signaling extraction.

T1—North American channelized TDM with 24 channels of 64 kHz each plus 8 kHz frame.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.

1-Port DSU/CSU T1 WIC for the Cisco 1700, Cisco 2600, Cisco 3600, and Cisco 3700 Series Routers

Feature History

Release	Modification
11.2	This feature was introduced on the Cisco 1600 series and Cisco 3600 series routers.
12. 2(15)ZL	Version 2 of this feature is introduced on the Cisco 1700, Cisco 2600, Cisco 3600 and Cisco 3700 series routers, and the Cisco ICS 7750 communications manager.

This feature module describes the 1-port data service unit/channel service unit (DSU/CSU) WAN interface card (WIC) for Cisco 1700, 2600, 3600, and 3700 series routers. It describes the benefits of the new feature, supported platforms, configuration, and related documents, and provides command reference information.

This document includes the following sections:

- Feature Overview
- Supported Platforms
- Supported Standards, MIBs, and RFCs
- Prerequisites
- Configuration Tasks
- Configuration Example
- Command Reference

Feature Overview

The Cisco WIC-1DSU-T1-V2 is an integrated, managed, T1 or fractional T1 WAN interface card (WIC). It provides nonchannelized data rates of 1 to 24 X 64 kbps or 1 to 24 X 56 kbps and follows ANSI T1.403 and AT&T Publication 62411 standards.

The Cisco WIC-1DSU-T1-V2 interface management features include the following:

- You can remotely configure the interface using Telnet and the Cisco IOS command line interface (CLI).
- For monitoring purposes, the router and DSU/CSU are manageable as a single Simple Network Management Protocol (SNMP) entity, using CiscoWorks or CiscoView. DSU/CSU statistics are accessed from the CLI.
- The SNMP agent supports the standard Management Information Base II (MIB II), Cisco integrated DSU/CSU MIB, and T1 MIB (RFC 1406).
- Loopbacks (including a manual button for a network line loopback) are provided for troubleshooting.
- Transmission attenuation can be tailored to cable length using the CLI.
- Test patterns, alarm counters, and performance reports are accessible using the CLI.
- The module has carrier detect, loopback, and alarm LEDs.

Benefits

This T1 DSU/CSU card works on the Cisco 1700, 2600, and 3600 series platforms, and allows customers to integrate more peripheral network components into the chassis. This is especially valuable to customers who deploy large scale, end-to-end Cisco-based branch networks.

Other benefits of this solution include the following:

- Fewer devices to deploy and manage
- Simplified management of the router
- DSU/CSU as a single entity
- Remote/local configuration, monitoring, and troubleshooting by using the CLI
- Single vendor support
- Enhanced reliability
- Physical space savings

Related Documents

Cisco Interface Card Documentation

- *Cisco Interface Card Installation Guide*
- *Quick Start Guide: Interface Cards for Cisco 1600 Series, Cisco 1700 Series, Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*

Cisco 1700 Series Routers Documentation

- *Cisco 1720 Router Hardware Installation Guide*

- *Quick Start Guide, Cisco 1720 Router*
- *Cisco 1721 Router Hardware Installation Guide*
- *Quick Start Guide, Cisco 1721 Router*
- *Cisco 1751 Router Hardware Installation Guide*
- *Cisco 1760 Router Hardware Installation Guide*
- *Quick Start Guide, Cisco 1760 Router*

Cisco 2600 Series Routers Documentation

- *Cisco 2600 Series Hardware Installation Guide*

Cisco 3600 Series Routers Documentation

- *Cisco 3600 Series Hardware Installation Guide*
- *Quick Start Guide, Cisco 3631 Router*

Cisco 3700 Series Routers Documentation

- *Cisco 3700 Series Routers Hardware Installation Guide*
- *Quick Start Guide, Cisco 3725 Router*
- *Quick Start Guide, Cisco 3745 Router*

Cisco ICS 7750 Documentation

- *ICS 7750 Documentation Roadmap*

Supported Platforms

This feature is supported on the following platforms:

- Cisco 1700 series routers
- Cisco 2600XM and Cisco 2691 routers
- Cisco 3631 routers
- Cisco 3700 series routers
- Cisco ICS 7750 communications manager

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 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

No new or modified MIBs are supported by this feature.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

The following are prerequisites to enable the T1 CSU WIC:

- Leased line from your telephone company
- Configuration parameters as specified by your telephone company. For most connections, the following default settings should suffice:
  - service-module t1 clock source line
  - service-module t1 data-coding normal
  - service-module t1 timeslots all speed 64
  - service-module t1 framing esf
  - service-module t1 lbo none
  - service-module t1 linecode b8zs
  - no service-module t1 remote-alarm-enable
  - no service-module t1 fdl

Note In telephone company initiated loopback tests that use the QRSS test pattern, the WIC-1DSU-T1-V2 *must* be clocked from the line. Configuring the WIC-1DSU-T1-V2 and the telephone company to use the same clock source will result in errors.

Note To view the current configuration, enter the **show service-module serial** *slot/port* command. For further information about these commands and how to change them, refer to the Cisco IOS configuration guides and command references.

Configuration Tasks

See the following sections for configuration tasks for this feature.

- Configuring Short Cable Transmission Attenuation
- Enabling Remote Loopback Testing

Configuring Short Cable Transmission Attenuation

To configure transmission attenuation for short cable lengths (under 660 feet in length), use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)#` **`interface serial0/0`**	Enter the interface configuration mode.
Step 2	`Router(config-if)#` **`service-module t1 cablelength short {110ft |220ft |330ft |440ft	550ft |660ft}`**	Optional. Sets the transmission attenuation according to the length of the cable. For example, use the keyword **110ft** if the cable length is from 0 to 110 feet. Use the keyword **220ft** if the cable length is from 110 to 220 feet, and so on.

Verifying Configuration of Short Cable Transmission Attenuation

To verify the configuration of short cable transmission attenuation, enter the EXEC command **show running-config interface serial**<*slot/port*> replacing <*slot/port*> with the slot and port number of the serial interface. The following sample output shows transmission attenuation for a cable length between 0 and 110 feet:

```
Router#show running-config interface serial0/0

Building configuration...

Current configuration : 252 bytes
!
interface Serial0/0
 no ip address
 load-interval 30
 no keepalive
 no fair-queue
 service-module t1 cablelength short 110ft
 service-module t1 framing sf
 service-module t1 linecode ami
 service-module t1 timeslots 1-24 speed 56
 no cdp enable
end
```

Enabling Remote Loopback Testing

To enable remote loopback testing for the WIC, use the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)#` **`interface serial0/0`**	Enter the interface configuration mode.
Step 2	`Router(config-if)#` **`service-module t1 remote-loopback {full | payload v54}`**	Optional. Specifies that the WIC-1DSU-T1-V2 card will enter loopback mode when it receives a loopback code on the line. The keywords are as follows: • **full**—enables standard loopup codes: 1-in-5 pattern for loopup mode and 1-in-3 pattern for loopdown mode. • **payload v54**—enables v54 pseudo-random loopup and loopdown codes for loopup and loopdown modes.

Verifying Enabling of Remote Loopback Testing

To verify the loopback status of the current interface, after the far end has been put in loopback mode, enter the command **show service-module serial**<*slot/port*> replacing <*slot/port*> with the slot and port number of the serial interface. The output "Unit is currently in test mode: remote loopback is in progress", as shown in the following example, indicate that remote loopback testing is enabled:

```
Router#show service-module serial0/0
Module type is T1/fractional
    Hardware revision is 0.1, Software revision is 20021210,
    Image checksum is 0x81277248, Protocol revision is 0.1
Receiver has no alarms.
Unit is currently in test mode:
    remote loopback is in progress
Framing is SF, Line Code is AMI, Current clock source is line,
Fraction has 24 timeslots (56 Kbits/sec each), Net bandwidth is 1344 Kbits/sec.
Last module self-test (done at startup): Passed
Last clearing of alarm counters 01:52:27
    loss of signal        :    1, last occurred 01:45:24
    loss of frame         :    2, last occurred 01:45:24
    AIS alarm             :    0,
    Remote alarm          :    0,
    Module access errors  :    0,
Total Data (last 7 15 minute intervals):
    255 Line Code Violations, 0 Path Code Violations
    1 Slip Secs, 326 Fr Loss Secs, 6 Line Err Secs, 0 Degraded Mins
    2 Errored Secs, 0 Bursty Err Secs, 7 Severely Err Secs, 327 Unavail Secs
Data in current interval (445 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 1 Severely Err Secs, 0 Unavail Secs
```

Configuration Example

This section provides a configuration example for a Cis co 1751 router with a WIC-1DSU-T1-V2 card installed. It is in a short cable environment (between 330 and 440 feet here), and is set to enter loopback when a loopback code is received on the line.

```
Current configuration :
!
version 12.2
no parser cache
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1751-uut1
!
interface Serial0/0
 ip address 10.0.0.51 255.0.0.0
 service-module t1 framing esf
 service-module t1 linecode b8zs
 service-module t1 timeslots 1-12 speed 64
 service-module t1 data-coding normal
 service-module t1 cablelength short 440ft
 service-module t1 remote-loopback full
!
interface FastEthernet0/0
 ip address 6.0.0.1 255.0.0.0
 speed auto
 full-duplex
!
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

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.

New Command

- **service-module t1 cablelength short**

Modified Command

- **service-module t1 remote-loopback**

NM-16A/S

The NM-16A/S is a slow-speed, high-density serial network module (NM) offering asynchronous and synchronous interfaces and flexible port configuration. The NM-16A/S offers:

- Synchronous interfaces that support a data rate of up to 128 kbps
- Asynchronous interfaces that support a data rate of up to 115.2 kbps
- Configurable data terminal equipment (DTE) and data circuit-terminating equipment (DCE)

Feature History for NM-16A/S

Release	Modification
12.2(15)ZJ	This feature was introduced.
12.3(2)T	This feature was integrated into Cisco IOS Release 12.3(2)T.

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 NM-16A/S

This feature requires Cisco IOS Release 12.2(15)ZJ or Release 12.3(2)T or a later release.

Restrictions for NM-16A/S

The NM-16A/S is factory configurable and not field upgradable.

Information About NM-16A/S

To configure the NM-16A/S feature, you must understand the following concept.

- Synchronous and Asynchronous Mode Configurations, page 518
- Platform Support for the NM-16A/S Feature, page 518

Synchronous and Asynchronous Mode Configurations

The synchronous ports are addressed as **interface serial** *slot*/*port*. The asynchronous port, when configured, utilizes the tty line numbering scheme, which is linear and allows for 32 tty ports per network module slot. Table 29 shows the port number corresponding to tty line number.

Table 29 Port Numbering Scheme

Slot Number	tty Terminal Line Number	Telnet TCP Port Number	Raw TCP Port Number	Binary TCP Port Number
0	1–32	2001–2032	4001–4032	6001–6032
1	33–64	2033–2064	4033–4064	6033–6064
2	65–96	2065–2096	4065–4096	6065–6096
3	97–128	2097–2128	4097–4128	6097–6128
4	129–160	2129–2160	4129–4160	6129–6160
5	161–192	2161–2192	4161–4192	6161–6192
6	193–224	2193–2224	4193–4224	6193–6224

Platform Support for the NM-16A/S Feature

This feature is supported on Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.

This feature is *not* supported on the non-XM models of the Cisco 2610, Cisco 2611, Cisco 2620, Cisco 2621, Cisco 2650, Cisco 2651. This feature is *not* supported on the Cisco 3620, Cisco 3640, and Cisco 3640/A routers.

How to Configure the NM-16A/S

This section contains the following procedures:

- Configuring the Slow-Speed Interfaces for NM-16A/S, page 519
- Configuring the ignore Command for NM-16A/S, page 522

Configuring the Slow-Speed Interfaces for NM-16A/S

To specify the mode of a slow-speed serial interface on a router as either synchronous or asynchronous, use the following commands:

SUMMARY COMMANDS

1. **enable**
2. **configure terminal**
3. **interface serial** *slot*/*port*
4. **physical-layer** {**sync** | **async**}
5. **clock rate** {*speed* | **line** *rate*}
6. **speed** *bps*
7. **ip address** *ip-address mask* [**secondary**]
8. **encapsulation** *encapsulation-type*
9. **load-interval** *seconds*
10. **exit**

DETAILED COMMANDS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface serial`** *`slot/port`*
	Example:
	`Router(config)# interface serial 1/1`
		Enters interface configuration mode and specifies the serial interface created on the controller.
		• *slot*/*port*—Backplane slot number and port number on the controller. The slash mark is required.

	Command or Action	Purpose

Step 4	**physical-layer** {**sync** | **async**}
	Example:
	`Router (config-if)# physical-layer async`
		Specifies the mode of a slow-speed serial interface.
		• **sync**—Places the interface in synchronous mode. This is the default.
		• **async**—Places the interface in asynchronous mode.

Step 5	**clock rate** {*speed* | **line** *rate*}
	Example:
	`Router (config-if)# clock rate 128000`
		Configures the clock rate for serial interfaces and interface processors to an acceptable bit rate.
		• *speed*—Desired clock rate in bits per second: 300, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 32000, 38400, 56000, 57600, 64000, 72000, 125000, or 128000.
		• Using the **line** keyword specifies the line clock.
		• The *rate* argument specifies the rate when the **line** keyword is used.
		• Must be configured on the DCE interface if the mode is synchronous.
		• To remove the clock rate if you change the interface from a DCE to a DTE device, use the **no** form of this command.
		• Using the **no** form of this command on a DCE interface sets the clock rate to the hardware-dependent default value.

Step 6	**speed** *bps* **Example:** `Router (config-if)# speed 115200`	(Optional) Configures the speed for an interface. • This is only for asynchronous mode; default is 9600 bps. • Configured only if a different speed is required. • Both interfaces at each end of the cable must be configured for the same speed. • To disable a speed setting, use the **no** form of this command.
Step 7	**ip address** *ip-address mask* [**secondary**] **Example:** `Router (config-if)# ip address 192.168.220.220 255.255.0.0 secondary`	Sets a primary or secondary IP address for an interface. • *ip-address*—IP address for the interface. • *mask*—Mask for the associated IP subnet. • **secondary**—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

	Command or Action	Purpose
Step 8	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface. • *encapsulation-type*—Encapsulation type; one of the following keywords: – **atm-dxi**—ATM Mode-Data Exchange Interface. – **bstun**—Block Serial Tunnelling. – **frame-relay**—Frame Relay (for serial interface). – **hdlc**—High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. – **isl**—Inter-Switch Link (ISL) (for virtual LANs). – **lapb**—X.25 Link Access Procedure, Balanced. Data link layer protocol (LAPB) DTE operation (for serial interface). – **ppp**—PPP (for serial interface). – **sdlc**—IBM serial Systems Network Architecture (SNA). – **sdlc-primary**—IBM serial SNA (for primary serial interface). – **sdlc-secondary**—IBM serial SNA (for secondary serial interface). – **slip**—Specifies Serial Line Internet Protocol (SLIP) encapsulation for an interface configured for dedicated asynchronous mode or dial-on-demand routing (DDR). This is the default for asynchronous interfaces. – **smds**—Switched Multimegabit Data Services (SMDS) (for serial interface). **Note** For more extensive information about the options for *encapsulation-type,* refer to the Cisco IOS Release 12.3 T Cisco IOS command references master index for the **encapsulation** command. This information is available on cisco.com.
Step 9	**load-interval** *seconds* **Example:** `Router(config-if)# load-interval 90`	Changes the length of time for which data is used to compute load statistics. • *seconds*—Length of time for which data is used to compute load statistics. A value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on).
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Configuring the ignore Command for NM-16A/S

Perform this task to configure the serial interface to ignore the specified signals as the line up/down indicator:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial** *slot*/*port*
4. **ignore** [**dtr** | **rts**]
   or
   ignore [**dtr** | **local-loopback** | **rts**]
   or
   ignore [**cts** | **dsr**]
   or
   ignore [**cts** | **dcd** | **dsr**]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`interface serial` *`slot`*`/`*`port`*
	Example:
	`Router(config)# interface serial 1/1`
		Specifies the serial interface created on the controller.
		• *slot*/*port*—Backplane slot number and port number on the controller. The slash mark is required.

	Command or Action	Purpose
Step 4	**ignore** [**dtr** | **rts**] or **ignore** [**dtr** | **local-loopback** | **rts**] or **ignore** [**cts** | **dsr**] or **ignore** [**cts** | **dcd** | **dsr**] **Example:** `Router(config-if)# ignore dtr`	For DCE asynchronous mode. or For DCE synchronous mode. or For DTE asynchronous mode. or For DTE synchronous mode. **Note** This command is disabled by default. The **no ignore** command restores the default. Specifies the serial signal to be ignored. • **dtr**—Specifies that the DCE ignores the data terminal ready (dtr) signal. • **rts**—Specifies that the DCE ignores the request to send (rts) signal. • **local-loopback**—Specifies that the DCE ignores the local loopback signal. • **cts**—Specifies that the DTE ignores the clear to send (cts) signal. • **dsr**—Specifies that the DTE ignores the data set ready (dsr) signal. • **dcd**—Specifies that the DTE ignores the data carrier detect (dcd) signal.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

What to Do Next

To verify that the slow-speed serial interface is configured correctly, enter the **show interfaces serial** privileged EXEC command to display the command settings for the router.

To enable the transition of the serial control leads to be reported on the console, use the **debug serial lead-transition** command in privileged EXEC mode.

Caution To avoid having the debug message flood the console screen with debug information, use these commands only when traffic on the IP network is low, so other activity on the system is not adversely affected.

The following is sample output from the **debug serial lead-transition** command:

```
Router# debug serial lead-transition
Router# debug condition interface serial 1/1

*Mar  1 00:17:15.040:slot(1) Port(1):DSR/DTR is Deasserted
*Mar  1 00:17:15.040:slot(1) Port(1):CTS/RTS is Deasserted

*Mar  1 00:17:47.955:slot(1) Port(1):DCD/Local Loop is Deasserted
*Mar  1 00:17:47.955:slot(1) Port(1):DSR/DTR is Deasserted
*Mar  1 00:17:47.955:slot(1) Port(1):CTS/RTS is Deasserted


Router# no shut down serial 1/1

*Mar  1 00:16:52.298:slot(1) Port(1):DSR/DTR is Asserted
*Mar  1 00:16:52.298:slot(1) Port(1):CTS/RTS is Asserted

*Mar  1 00:16:31.648:slot(1) Port(1):DCD/Local Loop is Asserted
*Mar  1 00:16:31.648:slot(1) Port(1):DSR/DTR is Asserted
*Mar  1 00:16:31.648:slot(1) Port(1):CTS/RTS is Asserted
```

Configuration Examples for NM-16A/S

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

- show running-config Example, page 524

show running-config Example

```
interface Serial1/0
 ip address 10.1.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/1
 ip address 10.2.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/2
 ip address 10.3.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/3
 ip address 10.4.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/4
 ip address 10.5.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/5
 ip address 10.6.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/6
 ip address 10.7.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/7
 ip address 10.8.0.2 255.255.255.0
 load-interval 30
 no keepalive
 clockrate 128000
 fair-queue
 no cdp enable
!
interface Serial1/8
 physical-layer async
 ip address 10.9.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
 fair-queue 64 16 0
!
interface Serial1/9
 physical-layer async
 ip address 10.10.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
 fair-queue 64 16 0
!
interface Serial1/10
 physical-layer async
 ip address 10.11.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
 fair-queue 64 16 0
!
interface Serial1/11
 physical-layer async
 ip address 10.12.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
 fair-queue 64 16 0
!
interface Serial1/12
 physical-layer async
 ip address 10.13.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
 fair-queue 64 16 0
!
interface Serial1/13
 physical-layer async
 ip address 10.14.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
 fair-queue 64 16 0
!
interface Serial1/14
 physical-layer async
 ip address 10.15.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
 fair-queue 64 16 0
!
interface Serial1/15
 physical-layer async
 ip address 10.16.0.2 255.255.255.0
 encapsulation ppp
 load-interval 60
 async mode dedicated
!
end
```

Additional References

The following sections provide references related to NM-16A/S.

Related Documents

Related Topic	Document Title
Basic information for configuration	*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide, Release 12.3*
Cisco IOS voice commands	*Cisco IOS Voice Command Reference,* Release 12.3 T
Configuration guidelines and detailed command reference information for voice, video, and fax	*Cisco IOS Voice Configuration Library*
Hardware installation instructions for network modules	*Connecting Serial Network Modules*

MIBs

MIBs	MIBs Link
• CISCO-ENTITY-VENDORTYPE-OID-MIB.my • OLD-CISCO-CHASSIS-MIB.my • ENTITY-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://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2515	*Definitions of Managed Objects for ATM Management.* K. Tesink, Ed.

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, tools, and lots more. 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 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.

- **clock rate**
- **debug serial lead-transition**
- **ignore (interface)**

Glossary

ATM—asynchronous transfer mode.

cts—clear to send. Circuit in the EIA/TIA-232 specification that is activated when DCE is ready to accept data from a DTE.

DCE—data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE. Compare with DTE.

dcd—data carrier detect. DCD is a signal from the DCE device that typically means that the DCE is ready to accept data. If the DCE device is a modem, the DCD signal traditionally refers to the modem having received a modulation carrier signal and is now able to pass data.

DDR—dial-on-demand routing.

dsr—data set ready. EIA/TIA-232 interface circuit that is activated when DCE is powered up and ready for use.

DTE—data terminal equipment. Device at the user end of a user-to-network interface that serves as a data source, destination, or both. DTE connects to a data network through a DCE device (for example, a modem) and typically uses clocking signals generated by the DCE. DTE includes such devices as computers, protocol translators, and multiplexers. Compare with DCE.

dtr—data terminal ready. EIA/TIA-232 circuit that is activated to let the DCE know when the DTE is ready to send and receive data.

HDLC—High-Level Data Link Control.

ISL—Inter-Switch Link.

LAPB—Link Access Procedure, Balanced.

NIM—network interface module.

PPP—Point-to-Point Protocol.

rts—request to send. EIA/TIA-232 control signal that requests a data transmission on a communications line.

SLIP—Serial Line Internet Protocol.

SMDS—Switched Multimegabit Data Services.

VIP—Versatile Interface Processor.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.

1-Port ADSL WAN Interface Card

Feature History

Release	Modification
12.1(3)XJ	This feature was introduced on the Cisco 1700 series routers.
12.2(2)T	This feature was integrated into Cisco IOS Release 12.2(2)T.
12.2(13)ZH	This feature was expanded to include the WIC-1ADSL-I-DG interface card on Cisco 1700 series modular access routers, to support ADSL over ISDN WAN. For specific platforms supported, see Table 30 on page 531.
12.2(15)ZJ	This feature was expanded to include the WIC-1ADSL-I-DG interface card on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series modular access routers. For specific platforms supported, see Table 30 on page 531.
12.3(4)T	Support was added for the WIC-1ADSL-I-DG interface card on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series modular access routers. For specific platforms supported, see Table 30 on page 531.

This feature module describes the 1-port Asymmetric Digital Subscriber Line (ADSL) Wide Area Network (WAN) Interface Card (WIC) feature. It describes the benefits of the feature, supported platforms, configuration, related documents, and provides command reference information.

This document includes the following sections:

Feature Overview

The Cisco ADSL WAN interface cards are 1-port WAN interface cards (WIC) for Cisco modular access routers. These cards provide high-speed ADSL digital data transfer between a single customer premises equipment (CPE) subscriber and a central office.

Note ADSL is a last-mile access technology that uses an asymmetrical data rate over a single copper wire pair.

The ADSL WICs are available in two variations: ADSL over POTS (WIC-1ADSL), and ADSL over ISDN WAN with Dying Gasp support (WIC-1ADSL-I-DG). The following bullets summarize the features of each card:

- Cisco WIC-1ADSL—Provides ADSL services over ordinary telephone lines. It is compatible with the Alcatel Digital Subscriber Loop Access Multiplexer (DSLAM), the Cisco 6260 DSLAM with Flexi-line cards, and the Cisco 6130 DSLAM with Flexi-line cards.
- Cisco WIC-1ADSL-I-DG—Provides_ADSL services in areas of the world that have extensive ISDN backbones already in place. It is compatible with ECI, Siemens, Alcatel, and Cisco DSLAMs that support ISDN.

All Cisco ADSL WICs support Asynchronous Transfer Mode (ATM) Adaptation Layer 2 (AAL2) for the Cisco 2600, Cisco 3600, and Cisco 3700 series only, and AAL5 for the those models as well as for the Cisco 1700. The cards support various classes of Quality of Service (QoS) for both voice and data.

Benefits

Both Cisco ADSL WAN interface cards provide the following benefits:

- Enable business-class broadband service with voice integration, scalable performance, flexibility, and security
- Aggregate both ADSL and other transport options into a single box
- Provide ADSL high-speed digital data transmissions between CPE and the central office (CO)
- Support ATM AAL5 services and applications, ATM class of service (constant bit rate [CBR], variable bit rate-nonreal time [VBR-NRT], variable bit rate–real time [VBR–rt], and unspecified bit rate [UBR]), as well as up to 23 virtual circuits on a WIC in Cisco routers
- Provide ATM traffic management and QoS features to enable service providers to manage their core ATM network infrastructure.

The following benefits are specific to each card:

- Cisco WIC-1ADSL—Supports and complies with ANSI T1.413 Issue 2, and ITU G.992.1, Annex A (G.DMT for full-rate ADSL over POTS)
- Cisco WIC-1ADSL-I-DG—Allows the coexistence of ADSL and ISDN on the same local loop; supports and complies with ITU G.992.1, Annex B (G.DMT for full-rate ADSL over ISDN), ETSI 101-388, and the Deutsche Telekom U-R2 specification

Restrictions

The Cisco ADSL WAN interface cards do not support dual latency, ADSL2, or ADSL2plus. When the ADSL link is intended to support both voice and data traffic simultaneously, the link should be configured for either all fast-path data or all interleave data, with an interleave depth of zero to ensure that latency is minimized. In addition, the total supported data rate must be reduced to adjust for the reduced coding gain, which is usually present with high-latency traffic.

Related Documents

- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.3(4)T*
- *Caveats for Cisco IOS Release 12.3 T*
- *Cisco Interface Cards Hardware Installation Guide*
- *Enhanced Voice and QoS for ADSL and G.SHDSL on Cisco 1700 Series, Cisco 2600 Series, and Cisco 3600 Series Routers*
- *Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers*

Supported Platforms

Table 30 details the specific platforms that each card supports.

Table 30 Platforms Supported by Each Cisco ADSL WAN Card

Cisco WIC-1ADSL	Cisco WIC-1ADSL-I-DG
Cisco 1720, Cisco 1721, Cisco 1751, Cisco 1760, Cisco 2600, Cisco 2600XM, Cisco 2691, Cisco 3600, Cisco 3700	Cisco 1721, Cisco 1751, Cisco 1760, Cisco 2600XM, Cisco 2691, Cisco 3700

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 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

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.

Configuring the Cisco ADSL WAN Interface Cards

This section documents the new or changed Cisco IOS commands for configuring the Cisco ADSL WAN Interface Card feature. All other commands used to configure that feature are documented in the following publications:

- *Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers*
- The "Configuring ATM" section of the *Cisco IOS Wide-Area Networking Configuration Guide*
- The "ATM Commands" section of the *Cisco IOS Wide-Area Networking Command Reference*

See the following sections for configuration information:

- Configuration Example, page 532
- Command Reference, page 533

Configuration Example

The following sample shows a Cisco 1700 series router configured for bridging on the ATM interface with a Cisco ADSL WIC:

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname meltrack
!
no ip routing
!
interface ATM0
no ip address
atm vc-per-vp 256
 pvc 8/35
 encapsulation aal5snap
!
dsl operating-mode auto
bridge-group 1
!
interface FastEthernet0
no ip address
speed auto
bridge-group 1
!
ip classless
no ip http server
!
bridge 1 protocol ieee
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Additional References

The following section provides a reference related to the ADSL WAN interface card.

Related Documents

Related Topic	Document Title
ADSL WAN interface card on Cisco 1700 series routers	*Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers*

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 Commands

- **dsl operating-mode**

Circuit Emulation over IP

Circuit Emulation over IP (CEoIP) provides a virtual circuit through an IP network—similar to a leased line—to integrate solutions that require a time-sensitive, bit-transparent transport into IP networks. Data, with proprietary framing or without, arrives at its destination unchanged; the transport is transparent to the destination.

Feature History for Circuit Emulation over IP

Release	Modification
12.3(7)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.

Contents

Prerequisites for Circuit Emulation over IP

- The CEoIP feature requires a CEoIP network module (NM) on each end of the connection, either the NM-CEM-4TE1 NM or the NM-CEM-4SER NM. You do not need to use the same type of CEoIP NM on both ends of the connection.

- The CEoIP feature requires 300 KB of flash memory and 1 MB of DRAM in addition to your Cisco IOS software requirements.

Restrictions for Circuit Emulation over IP

- NM-CEM-4TE1 supports only B8ZS (T1) and HDB3 (E1) line codes.
- E1 lines do not support 56 kbps connections.
- CEoIP software cannot run payload compression for more than 3.088 Mbps) per network module.
- If you configure four T1, E1, or serial cables (over 1.544 M) at the same time in Cisco 2600XM series routers, you cannot turn on the data-protection and payload compression features. Also, in framed mode (channelized), you can use up to 60 channels without the data protection and payload compression features on Cisco 2600XM series routers. However, you can turn on the data protection and payload compression feature in one T1/E1.
- There is a limitation on the data protection and payload compression features on Cisco 3660 routers. If you configure four T1, E1, or serial cables on Cisco 3660 routers, you can turn on data protection for up to two T1/E1s. In framed mode, you can use 88 channels.

Information About Circuit Emulation over IP

To configure Circuit Emulation over IP, you should understand the following concepts:

Circuit Emulation over IP

Circuit emulation is an end-to-end service that allows Layer 1 data to be transported transparently through an IP network. Applications that require circuit emulation need the network to provide a constant rate bit stream.

CEoIP may use adaptive clocking as a means of synchronizing the clock frequencies at the two endpoints. Channel associated signaling (CAS) transport is provided as an optional feature to allow channelized voice applications. Payload compression is provided as an optional feature to improve bandwidth efficiency and data protection is provided to reduce the probability of data loss.

CEoIP software supports the following network modules:

- The NM-CEM-4SER, a network module with four serial ports. To configure CEoIP software for the NM-CEM-4SER, you must configure the options of the ports. Options include dejitter buffer, payload compression, and payload size.
- The NM-CEM-4TE1, a network module with four ports that you can configure as T1 or E1 (where all four ports support the same interface type). To configure CEoIP software for the NM-CEM-TE1, you must define the card type and then configure the options of the port.

Benefits of CEM over IP

CEoIP provides a simple migration path to IP-only networks. Examples of solutions that CEoIP integrates with IP include the following:

- Legacy data services
- Legacy video applications
- Satellite data streams
- Radar data streams
- Telemetry for automated industrial environments (for example, power distribution)
- Crypto tunneling for multilevel security

Adaptive Clocking for CEoIP

The adaptive clocking option of CEoIP allows the egress clock to vary by expanding or contracting the clock period from the nominal clock. After you have implemented the clocking feature, the adaptive clocking circuits continuously adjust the selected clock based on the data buffer level. You can implement adaptive clocking on each port independently.

Payload Compression for CEoIP

The payload compression option minimizes the amount of bandwidth that traffic consumes. It compresses the transmission of any repetitive data pattern (for example, idle code, HDLC flags, and so on) to increase the efficiency of the solution across the network.

With CEoIP software, you can adjust the size (in bytes) of the payload for the IP packet to configure efficiency as opposed to packetization. Larger payloads provide more efficiency but increase the delay. With smaller packets the overhead of the header increases. Payload compression is disabled by default.

Data Protection (Sample Repetition)

The data protection option, also known as sample repetition, reduces the probability of errors due to packet loss by sending each sample twice, in two different IP packets. Data protection consumes more bandwidth than standard transmission, but you can minimize the amount of traffic with payload compression. This feature is disabled by default.

Dejitter

The dejitter buffer size determines the ability of the emulated circuit to tolerate network jitter. The dejitter buffer in CEoIP software is configurable up to 500 milliseconds; the maximum amount of network jitter that CEoIP can tolerate is ±250 milliseconds.

Idle Pattern

The idle pattern option specifies the idle pattern to transmit when the circuit goes down. You can specify a maximum of 64 bits with two 32-bit patterns for the NM-CEM-4SER and 8-bit patterns for the NM-CEM-4TE1.

Payload Size

Payload size is the number of bytes put into each IP packet. This parameter impacts packetization delay and efficiency. Configure a high payload size to increase packetization delay and efficiency. A smaller payload size reduces packetization delay and efficiency.

Signaling for CEoIP

CEoIP software supports the transport of channel associated signaling (CAS) bits in channelized T1/E1 mode. This option extracts incremental signaling information and sends that information in separate packets.

Control Lead Configurations

CEoIP software supports the monitoring and transport of serial interface control leads.

How to Configure Circuit Emulation over IP

This section contains the tasks for configuring an NM-CEM-4TE1 and an NM-CEM-4SER.

To configure an NM-CEM-4TE1, go to the "Configuring the NM-CEM-4TE1 Card Type" section on page 539.

To configure an NM-CEM-4SER, go directly to the "Configuring the Connection Using the xconnect Command" section on page 544.

- Configuring the NM-CEM-4TE1 Card Type, page 539
- Configuring the T1/E1 Line, page 539
- Creating CEM Channels on the T1/E1 Line, page 543
- Configuring the Connection Using the xconnect Command, page 544
- Configuring the CEM Channel, page 546

Configuring the NM-CEM-4TE1 Card Type

Perform this task to configure the card type for an NM-CEM-4TE1.

This task does not apply to the NM-CEM-4SER.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **card type** {**t1** | **e1**} *slot*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**card type** {**t1** | **e1**} *slot* **Example:** `Router(config)# card type t1 1`	Configures the card type by specifying the transmission mode for the ports on the network module. • All four ports on the CEoIP T1/E1 network module must operate in the same mode. • Use the **t1** or **e1** keyword to specify the transmission mode for all four ports. **Note** This command is only entered once and changes do not take effect unless the **reload** command is used, or the router is rebooted.

What to Do Next

Go to the "Configuring the T1/E1 Line" section on page 539 to continue configuring CEoIP on an NM-CEM-4TE1.

Configuring the T1/E1 Line

Perform this task to configure the T1 or E1 line, starting in global configuration mode.

This task does not apply to the NM-CEM-4SER.

SUMMARY STEPS

1. **controller** {**t1** | **e1**} *slot*/*port*
2. **framing** {**esf** | **sf** | **unframed**}
   or
   framing {**crc4** | **no-crc4** | **unframed**}
3. **clock source** {**internal** | **line** | **adaptive** *channel-number*}
4. **cablelength** {**long** | **short**} {*attenuation* | *length*}
5. **crc-threshold** *value*
6. **description** *text*
7. **loopback**{**local** {**line** | **payload**} | **network**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller** {**t1** | **e1**} *slot*/*port* **Example:** `Router(config)#` **`controller t1 1/0`**	Enters controller configuration mode. • Use the *slot* and *port* arguments to specify the slot number and port number to be configured.

Step 2	**framing** {**esf** | **sf** | **unframed**}
	or
	framing {**crc4** | **no-crc4** | **unframed**}
	
	Example:
	`Router(config-controller)#` **`framing esf`**
	
	Example:
	`Router(config-controller)#` **`framing crc4`**
		(Optional) Configures the framing format for a T1 or E1 port to synchronize the port and the attached device.
		
		T1 port framing options:
		• Use the **esf** keyword to specify Extended Superframe as the T1 framing type.
		• Use the **sf** keyword to specify the Superframe (also commonly called D4 framing) as the T1 framing type. This is the default.
		
		E1 port framing options:
		• Use the **crc4** keyword to specify the G.704 standard with optional CRC4 mechanism defined in timeslot zero (0) enabled as the E1 framing type. This is the default.
		• Use the **no-crc4** keyword to specify the G.704 standard with optional CRC4 mechanism defined in timeslot zero (0) disabled as the E1 framing type.
		
		T1 or E1 port framing options:
		• Use the **unframed** keyword to specify the unchannelized mode of framing.
		Note If you do not configure framing, the framing on the customer premises equipment (CPE) devices on each end of the connection must match.

	Command or Action	Purpose

Step 3	**`clock source`** `{`**`internal`** `|` **`line`** `|` **`adaptive`** *`channel-number`*`}`
	Example:
	`Router(config-controller)#` **`clock source adaptive 6`**
		Configures the clock source for a T1 or E1 port.
		• Use the **internal** keyword to specify that the port transmit clock is derived from the time-division multiplexing (TDM) bus backplane clock, if one exists in the router, or the on-board oscillator on the network module.
		• Use the **line** keyword to specify that the port transmit clock is derived from the the receive clock on the same port.
		• Use the **adaptive** keyword to specify that the port transmit clock is locally synthesized based on the average data content of the dejitter buffer of one of the channels on this port.
		• If the **adaptive** keyword is selected, use the *channel-number* argument to specify the channel whose dejitter buffer is to be used to synthesize the transmit clock of the port.

Step 4	**`cablelength`** `{`**`long`** `|` **`short`**`}` `{`*`attenuation`* `|` *`length`*`}`
	Example:
	`Router(config-controller)#` **`cablelength long -15db`**
		(Optional) Specifies the line build-out characteristics of the internal CSU on a T1 port.
		• Use the **long** keyword to specify that the signal characteristics are set for a long cable length.
		• Use the **short** keyword to specify that the signal characteristics are set for a short cable length.
		• If the **long** keyword is selected, use the *attenuation* argument to specify the T1 signal attenuation.
		• If the **short** keyword is selected, use the *length* argument to specify the T1 cable length.
		Note This command does not apply to an E1 port.

Step 5	**`crc-threshold`** *`value`*
	Example:
	`Router(config-controller)#` **`crc-threshold 512`**
		(Optional) Configures the number of cyclical redundancy check (CRC) errors in one second that results in the second being declared as a Severely Errored Second (SES).
		• Use the *value* argument to specify the number of CRC errors. Default is 320.
		Note This command does not apply to an E1 port.

	Command or Action	Purpose

Step 6	`description text`
	Example:
	`Router(config-controller)# description T1 line to 3rd floor PBX`
		(Optional) Specifies a text description of the port.

Step 7	`loopback {local {line | payload}| network}`
	Example:
	`Router(config-controller)# loopback network`
		(Optional) Creates a loopback from a T1 or E1 port.
		• Use the **local** keyword to create a loopback where the information from a locally-attached CPE is transmitted back to the locally-attached CPE.
		• Use the **network** keyword to create a loopback where the data received over the network from a remotely-attached CPE is transmitted back to the remotely-attached CPE.
		• If the **local** keyword is selected, use the **line** keyword to create a full physical layer loopback of all bits, including data and framing.
		• If the **local** keyword is selected, use the **payload** keyword to create a loopback of the data in the individual timeslots only. In this mode, framing bits are terminated on entry and regenerated on exit instead of being looped back. This mode is not available if the port is configured for **framing unframed**.

What to Do Next

Go to the "Creating CEM Channels on the T1/E1 Line" section on page 543 to continue configuring CEoIP on an NM-CEM-4TE1

Creating CEM Channels on the T1/E1 Line

Perform this task to create CEM channels on the T1 or E1 line, starting in controller configuration mode.

This task does not apply to the NM-CEM-4SER.

SUMMARY STEPS

1. **cem-group** *group-number* {**unframed** | **timeslots** *timeslot* [**speed** {**56** | **64**}]}
2. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**cem-group** *group-number* {**unframed** | **timeslots** *timeslot* [**speed** {**56** | **64**}]}
	Example:
	`Router(config-controller)# cem-group 6 timeslots 1-4,9,10 speed 64`
		Creates a circuit emulation channel from one or more timeslots of a T1 or E1 line of an NM-CEM-4TE1.
		• The *group-number* keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0-23. For E1 ports, the range is 0-30.
		• Use the **unframed** keyword to specify that a single CEM channel is being created including all timeslots and the framing structure of the line.
		• Use the **timeslots** keyword and the *timeslot-range* argument to specify the timeslots to be included in the CEM channel. The list of timeslots may include commas and hyphens with no spaces between the numbers, commas, and hyphens.
		• Use the **speed** keyword to specify the speed of the channels by specifying the number of bits of each timeslot to be used. This keyword applies only to T1 channels.

Step 2	**exit**
	Example:
	`Router(config-controller)# exit`
	`Router(config)#`
		Exits controller configuration mode and returns to global configuration mode.

What to Do Next

Go to the "Configuring the Connection Using the xconnect Command" section on page 544 to continue configuring CEoIP on an NM-CEM-4TE1

Configuring the Connection Using the xconnect Command

Perform this task to create a connection using the **xconnect** command, starting in global configuration mode. This task applies to configuring CEoIP on both the NM-CEM-4TE1 and the NM-CEM-4SER.

Note To properly configure the CEoIP feature, two CEoIP network modules must use the same UDP port number to communicate.

SUMMARY STEPS

1. **cem** *slot/port/channel*
2. **xconnect** *remote-ip-address virtual-connect-ID* **encapsulation** *encapsulation-type*
3. **local ip address** *ip-address*
4. **local udp port** *port-number*

5. **remote udp port** *port-number*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`cem slot/port/cem-group`
	Example:
	`Router(config)# cem 3/1/0`
		Enters CEM configuration mode to configure CEM channels.
		• Use the *slot* argument to specify the slot number in which the network module is installed.
		• Use the *port* argument to specify the port number of the CEM channel to be configured.
		• Use the *channel* argument to specify the CEM channel number to be configured. For a serial channel enter zero. For a T1 or E1 channel enter the channel number defined in the **cem-group** command (see the "Creating CEM Channels on the T1/E1 Line" section on page 543).

Step 2	`xconnect remote-ip-address virtual-connect-ID encapsulation encapsulation-type`
	Example:
	`Router(config-cem)# xconnect 10.2.0.1 0 encapsulation udp`
		Creates one end of a connection between two CEM network modules and enters xconnect configuration mode.
		• Use the *remote-ip-address* argument to specify the IP address of an interface—regular or loopback—on the destination router.
		• Set the *virtual-connect-ID* argument to be zero.
		Note Currently the only supported encapsulation type is UDP.

Step 3	`local ip address local-ip-address`
	Example:
	`Router(config-cem-xconnect)# local ip-address 10.2.0.2`
		Configures the IP address of an interface—regular or loopback—on the source router.
		Note The local IP address must be the same as the remote IP address (at the other side) configured in the **xconnect** command.

Step 4	`local udp port udp-port`
	Example:
	`Router(config-cem-xconnect)# local udp port 15901`
		Specifies the User Datagram Protocol (UDP) port number of the local CEM channel.
		Note The local UDP port of a CEM channel must be the same as the remote UDP port of the CEM channel at the other end of the connection.

	Command or Action	Purpose

Step 5	`remote udp port` *`udp-port`*
	Example:
	`Router(config-cem-xconnect)# remote udp port 15902`
		Specifies the UDP port number of the remote CEM channel.
		Note The remote UDP port of a CEM channel must be the same as the local UDP port of the CEM channel at the other end of the connection.

Step 6	`exit`
	Example:
	`Router(config-cem-xconnect)# exit`
	`Router(config-cem)#`
		Exits xconnect configuration mode and returns to CEM configuration mode.
		• Repeat this command if you wish to exit CEM configuration mode return to global configuration mode.

What to Do Next

This task must be repeated on the other CEM network module and each end of the CEM connection must be configured identically to allow traffic to pass between the network modules. When both network modules have been configured, continue to the "Configuring the CEM Channel" section on page 546.

Configuring the CEM Channel

Perform this task to configure the CEM T1/E1 or serial channel, starting in CEM configuration mode.

SUMMARY STEPS

1. **clock rate** *rate*
2. **clock mode** {**normal** | **split**}
3. **clock source** {**internal** | **loop** | **adaptive**}
4. **payload-size** *size*
5. **dejitter-buffer** *size*
6. **control-lead sampling-rate** *rate*
7. **control-lead state** {**active** | **fail**} *output-lead* {**on** | **off** | **follow**} [{**local** | **remote**} *input-lead*]
8. **data-strobe** *input-lead-name* {**on** | **off**}
9. **idle-pattern** *length pattern1* [*pattern2*]
10. **signaling**
11. **payload compression**
12. **data protection**
13. **ip dscp** *dscp*
14. **ip tos** *tos*
15. **ip precedence** *precedence*
16. **loopback** {**local** | **network**}
17. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`clock rate`** *`rate`*
	Example:
	`Router(config-cem)#` **`clock rate 38400`**
		(Optional) For serial channels only. Specifies the nominal bit rate of a serial CEM channel.
		• Use the *rate* argument to specify the data rate of the channel in bps. Default is 64000.

Step 2	**`clock mode`** `{`**`normal`** `|` **`split`**`}`
	Example:
	`Router(config-cem)#` **`clock mode split`**
		(Optional) For serial channels only. Specifies the clock mode of a serial CEM channel.
		• Use the **normal** keyword to specify that the Data Circuit-terminating Equipment (DCE) provides both the Receive Clock (RxC) and the Transmit clock (TxC) to the attached Data Terminal Equipment (DTE).
		• Use the **split** keyword to specify that the DCE provides the Receive Clock (RxC) to the attached DTE, and the DTE provides the external Transmit Clock (XTC or TT) to the DCE.
		Note Depending on the serial cable attached to the port, the port is automatically configured as either a DCE or DTE.

Step 3	**`clock source`** `{`**`internal`** `|` **`loop`** `|` **`adaptive`**`}`
	Example:
	`Router(config-cem)#` **`clock source loop`**
		(Optional) Configures the clock source for a serial CEM channel.
		• This step applies only to configuring serial channels. For information about configuring the clock source for T1 or E1 ports, see the "Configuring the T1/E1 Line" section on page 539.
		• Use the **internal** keyword to specify that the clock(s) provided by the network module to the CPE is derived from the TDM bus backplane clock, if one exists in the router, or the on-board oscillator on the network module.
		• Use the **loop** keyword to specify that the clock provided by the network module to the CPE is derived from the the clock receive from the CPE on the same port.
		• Use the **adaptive** keyword to specify that the clock(s) provided by the network module to the CPE is locally synthesized based on the average data content of the local dejitter buffer.
		Note The **loop** keyword is valid only when the **clock mode split** command is configured.

	Command or Action	Purpose
Step 4	**payload-size** *size* **Example:** Router(config-cem)# **payload-size 512**	(Optional) Specifies the number of bytes encapsulated into a single IP packet. • Use the *size* argument to specify the number of bytes included in the payload of each packet. Default is 32 bytes for a serial CEM channel. • For more information about T1 and E1 default values, see the **payload-size** command in the "Command Reference" section.
Step 5	**dejitter-buffer** *size* **Example:** Router(config-cem)# **dejitter-buffer 80**	(Optional) Specifies the size of the dejitter buffer used to compensate for the network filter. • Use the *size* argument to specify the size of the buffer in milliseconds. Default is 60.
Step 6	**control-lead sampling-rate** *rate* **Example:** Router(config-cem)# **control-lead sampling-rate 10**	(Optional) Specifies the sampling rate of input control leads on a serial CEM channel. • This command is used only on serial channels. • Use the *rate* argument to specify the frequency with which the control leads are sampled, in samples per second. Default is 0. **Note** Control lead update packets are independent of the data packets from the same channel.
Step 7	**control-lead state** {**active** | **fail**} *output-lead* {**on** | **off** | **follow**} [{**local** | **remote**} *input-lead*] **Example:** Router(config-cem)# **control-lead state active rts follow remote cts**	(Optional) Specifies the state of each output control lead on a serial CEM channel. • This command is used only on serial channels. • Use the **active** keyword to specify the state of the control lead when the connection is active. • Use the **fail** keyword to specify the state of the control lead when the connection has failed. • Use the *output-lead* argument to specify the name of the control lead. • Use the **on** keyword to specify that the control lead is permanently asserted. • Use the **off** keyword to specify that the control lead is permanently not asserted. • Use the **follow** keyword to specify that the control lead is to follow any changes in the state of an input control lead specified by the **local** or **remote** keywords and the *input-lead* argument. • Use the *input-lead* argument to specify the name of the local or remote control lead to follow. **Note** Control lead update packets are independent of the data packets for the same channel. **Note** The **control-lead sampling-rate** parameter must be set to non-zero for this feature to operate.

	Command or Action	Purpose

Step 8	**data-strobe** *input-lead* {**on** | **off**}
	Example:
	`Router(config-cem)# data-strobe dtr on`
		(Optional) Specifies that an input control lead is to be monitored and data is packetized and sent only when the specified control lead is in the specified state.
		• This command is used only on serial channels.
		• Use the *input-lead* argument to specify the input control lead to be monitored to determine whether input data is to be packetized.
		• Use the **on** keyword to specify that data packets are to be sent from this CEM channel only when the specified input lead is asserted.
		• Use the **off** keyword to specify that data packets are to be sent from this CEM channel only when the specified input lead is not asserted.
		• Use this command to save bandwidth when the attached CPE is inactive.
		Note Control lead update packets are still sent even if data packets are withheld.

Step 9	**Cisco NM-CEM-4SER:**
	idle-pattern *length pattern1* [*pattern2*]
	Cisco NM-CEM-4TE1:
	idle-pattern *pattern1*
	Example:
	Cisco NM-CEM-4SER:
	`Router(config-cem)# idle-pattern 53 0x12345678 0x87654321`
	Cisco NM-CEM-4TE1:
	`Router(config-cem)# idle-pattern 0x66`
		(Optional) Defines the idle data pattern to send to the attached CPE when packets are lost or the de-jitter buffer experiences an under-run condition.
		For serial CEM channels:
		• A bit pattern up to 64 bits long may be specified.
		• Use the *pattern1* argument to specify up to 32 bits of the least significant bits of the idle data pattern, in hex notation. Default is 0xFF.
		• Use the *pattern2* argument to specify the most significant bits of the idle data pattern, in hex notation. If the *length* argument is 32 bits or less, this argument is not permitted.
		• Use the *length* argument to specify the total length of the repeating bit pattern. Default is 8 bits.
		For T1 or E1 CEM channels:
		• An eight-bit pattern is specified.

Step 10	**signaling** **Example:** `Router(config-cem)# signaling`	(Optional) Enables the transport of Channel Associated Signaling (CAS) bits. **Note** This command applies only to framed T1 or E1 data channels.
Step 11	**payload-compression** **Example:** `Router(config-cem)# payload-compression`	(Optional) Enables payload compression on a CEM channel. **Note** Enabling payload compression adds a delay equal to one packet time.

	Command or Action	Purpose

Step 12	**`data-protection`**
	Example:
	`Router(config-cem)#` **`data-protection`**
		(Optional) Enables data protection by transmitting each data bit twice, once in each of two consecutive data packets.
		• Use the **data-protection** command to protect transmissions from the effects of lost IP packets.
		Caution Use this command carefully because it increases the network bandwidth used by the CEM connection.

Step 13	**`ip dscp`** *`dscp`*
	Example:
	`Router(config-cem)#` **`ip dscp 36`**
		(Optional) Configures the IP Differentiated Service Code Point (DSCP) for packets originating from this CEM channel.
		• Use the *dscp* argument to specify the value placed in the DSCP field of IP packets originating from this channel. Default is 46.
		Note If DSCP is configured, the **ip tos** and **ip precedence** commands are not available because they are mutually exclusive.

Step 14	**`ip tos`** *`tos`*
	Example:
	`Router(config-cem)#` **`ip tos 11`**
		(Optional) Configures the IP type of service (ToS) bits for the CEM channel.
		• Use the *tos* argument to specify the value placed in the ToS field of IP packets originating from this channel. Default is 5.
		Note If DSCP is configured, the **ip tos** command is not available because they are mutually exclusive.

Step 15	**`ip precedence`** *`precedence`*
	Example:
	`Router(config-cem)#` **`ip precedence 7`**
		(Optional) Configures the IP precedence bits for the CEM channel.
		• Use the *precedence* argument to specify the value placed in the precedence field of IP packets originating from this channel. Default is 0.
		Note If DSCP is configured, the **ip precedence** command is not available because they are mutually exclusive.

	Command or Action	Purpose

Step 16	**loopback** {**local** | **network**}
	Example:
	`Router(config-cem)# loopback network`
		(Optional) Creates a loopback from a CEM serial channel.
		• Use the **local** keyword to create a loopback where the information from a locally-attached CPE is transmitted back to the locally-attached CPE.
		• Use the **network** keyword to create a loopback where the data received over the network from a remotely-attached CPE is transmitted back to the remotely-attached CPE.
		Note For configuring a loopback on a T1 or E1 port, see the "Creating CEM Channels on the T1/E1 Line" section on page 543.

Step 17	**exit** **Example:** `Router(config-cem)# exit`	Exits CEM configuration mode and returns to global configuration mode. • Use this command one more time to exit to privileged EXEC mode.

What to Do Next

Proceed to the "Configuration Examples for CEoIP" section on page 551.

Configuration Examples for CEoIP

This section provides the following configuration examples:

- Configuring a T1 CEM Network Module: Example, page 551

Configuring a T1 CEM Network Module: Example

The following example shows a basic configuration of a T1 network module to configure the CEoIP feature.

```
card type t1 0
controller t1 4/0
 cem-group 6 timeslots 1-4,9,10 speed 64
 framing esf
 linecode b8zs
 clock source adaptive 6
 cablelength long -15db
 crc-threshold 512
 description T1 line to 3rd floor PBX
 loopback network
 no shutdown
 exit
cem 2/1/6
 xconnect 10.2.0.1 0 encapsulation udp
 local ip-address 10.2.0.9
 local udp port 15901
 remote udp port 15901
 payload-size 512
 dejitter-buffer 80
 signaling
exit
```

Additional References

For additional information related to the CEoIP feature, refer to the following references:

Related Documents

Related Topic	Document Title
CEoIP NMs	*Release Notes for Cisco NM-CEM-4TE1 and NM-CEM-4SER Network Module Software*

Standards

Standards	Title
GR-1089	*Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment*
GR-63	*Network Equipment-Building System (NEBS) Requirements: Physical Protection*
TIA/EIA-IS-968	*Technical Requirements for Connection of Terminal Equipment to the Telephone Network*

MIBs

MIBs	MIBs Link
• OLD-CISCO-CHASSIS-MIB • RFC1406-MIB • CISCO-ENTITY-VENDORTYPE-OID-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1406	*Definitions of Managed Objects for the DS1 and E1 Interface Types*
RFC 2495	*Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types* **Note** CEoIP supports RFC2495 to the same extent as IOS supports this RFC.

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 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.

- **cem**
- **cem-group**
- **clear cem**
- **clock mode**
- **clock source (CEM)**
- **control-lead sampling-rate**
- **control-lead state**
- **crc-threshold**
- **data-protection**
- **data-strobe**
- **default (CEM)**
- **dejitter-buffer**
- **framing (CEM)**
- **idle-pattern**
- **ip dscp**
- **local ip address**
- **local udp port**
- **loopback (CEM)**
- **payload-compression**
- **payload-size**
- **remote udp port**
- **show cem**
- **signaling**
- **xconnect (CEM)**

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:

- How to Configure Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source, page 558
- Verifying Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source Configuration, page 566
- Additional References, page 568
- Command Reference, page 569

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 31 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.

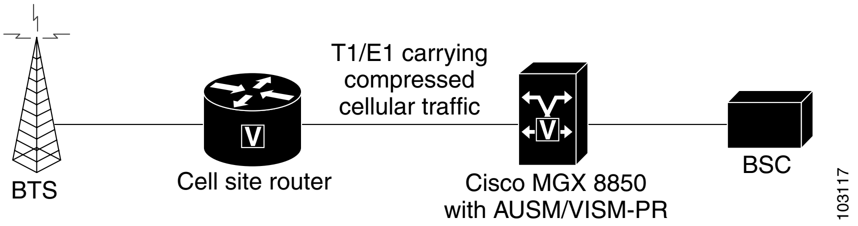
- ATM cell switching is limited to a maximum of 25 connections per AIM-ATM.
- Do not configure more than 29 LLCC channels per NM-HDV module. Configuring more than 29 LLCC channels can cause unreliable operation.
- J1 controller is not supported.
- Traffic policing is not supported.
- For Cisco 3660 routers 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 52 shows a sample topology that makes use of the Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source features.

Figure 52 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.

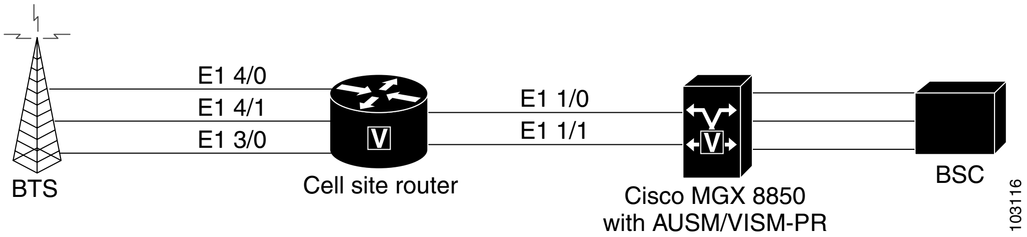
How to Configure Lossless Compression R1, ATM Cell Switching, and External BITS Clocking Source

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 559
- Configuring ATM Cell Switching, page 560
- Configuring the Lossless Compression Codec, page 562
- Disabling Connection Admission Control, page 565

The instructions that follow refer to the sample configuration shown in Figure 53. 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 53 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)**

Network Analysis Module (NM-NAM)

The Network Analysis Module (NM-NAM) feature is a network module that monitors and analyzes network traffic for a system using extended Remote Monitoring (RMON) standards, RMON2, and other Management Information Bases (MIBs).

Note The Network Analysis Module (NAM) is available in multiple hardware forms for some Cisco routers and Catalyst switches. This document applies only to the NAM for branch routers, also known as modular access, multiservice, or integrated services routers.

NAM provides Layer 2 to Layer 7 visibility into network traffic for remote troubleshooting, real-time traffic analysis, application performance monitoring, capacity planning, and managing network-based services, including quality of service (QoS) and Voice over IP (VoIP). The NAM Traffic Analyzer is software that is embedded in the NM-NAM that gives you browser-based access to the RMON1, RMON2, DSMON, and voice monitoring features of the NAM.

Feature History for NM-NAM

Release	Modification
12.3(4)XD	This feature was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This feature was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This feature was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This feature was implemented on the Cisco 3800 series.

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 the Network Analysis Module (NM-NAM)

- Install Cisco IOS Release 12.3(4)XD, Cisco IOS Release 12.3(7)T, or a later release.
- Install the NM-NAM network module. Make sure that the network module is properly seated and that the EN (enable) and PWR (power) LEDs come on. Refer to the *Cisco Network Modules Hardware Installation Guide*.
- For Cisco 2691, Cisco 3725, and Cisco 3745 routers only, make sure that the router runs ROM Monitor (ROMMON) Version 12.2(8r)T2 or a later version. This ROMMON version contains a fix that prevents the router from resetting all the network modules when it is reloaded. Refer to the *ROM Monitor Download Procedures for Cisco 2691, Cisco, 3631, Cisco 3725, and Cisco 3745 Routers*.

Restrictions for the Network Analysis Module (NM-NAM)

General Restrictions

- Cisco IOS Release 12.3(4)XD, Cisco IOS Release 12.3(7)T, or a later release is required.
- Network Analysis Module Release 3.2 or a later release is required.
- Only one NM-NAM can be installed in the router at any time.
- SNMPv3 is not supported.
- Online insertion and removal (OIR), or hot swapping network modules, is supported on some platforms. To find out if your router supports hot swapping, refer to the *Network Modules Quick Start Guide*.

Traffic Monitoring Restrictions for the Internal NAM Interface

The following restrictions apply only to traffic that is monitored through the internal NAM interface:

- Only IP traffic can be monitored.
- The NAM Traffic Analyzer (web GUI) provides Layer 3 and higher layer information about the original packets. The Layer 2 header is modified by the router when it forwards the packets to the NAM, so the Layer 2 information that the NAM records is not applicable to the original packets.
- When Network Address Translation (NAT) is used, the router forwards packets containing the NAT “inside” network addresses to the NAM.

- When access control lists are used:
  - Packets dropped by an inbound access list are not forwarded to the NAM.
  - Packets dropped by an outbound access list are forwarded to the NAM for analysis.
- The NAM does *not* monitor the following:
  - Packets that are dropped by the Cisco IOS because of errors
  - Outbound IP multicast, IP broadcast, and User Datagram Protocol (UDP) flooding packets
  - Packets in generic routing encapsulation (GRE) tunnels

Note The previous restrictions (in the "Traffic Monitoring Restrictions for the Internal NAM Interface" section) do not apply to traffic monitored through the external NAM interface.

Information About the Network Analysis Module (NM-NAM)

To configure and manage the NM-NAM, you should understand the following concepts:

- NM-NAM Hardware, page 573
- NAM User Interfaces, page 574
- NAM Network Interfaces, page 575
- NM-NAM Operating Topologies and IP Address Assignments, page 576
- NAM CLI, page 581

Note For NM-NAM features and benefits, supported hardware and software, and other product information, refer to the *Cisco Branch Router Network Analysis Module Data Sheet*.

NM-NAM Hardware

For information on hardware installation and cable connections, refer to the *Cisco Network Modules Hardware Installation Guide*.

Specifications

Table 32 NM-NAM Specifications

Specification	Description
Processor	500 Mhz Intel Mobile Pentium III
SDRAM	256 MB
Internal disk storage	NM-NAM 20 GB IDE
Dimensions (H x W x D)	1.55 x 7.10 x 7.2 in. (3.9 x 18.0 x 19.3 cm)
Weight	1.5 lb (0.7 kg) (maximum)
Operating temperature	3° to 104°F (0° to 40°C)

Table 32 NM-NAM Specifications (continued)

Specification	Description
Nonoperating temperature	–40° to 185°F (–40° to 85°C)
Humidity	5 to 95% noncondensing
Operating altitude	0 to 10,000 ft (0 to 3,000 m)

Faceplate and LEDs

Figure 54 NM-NAM Faceplate and LEDs

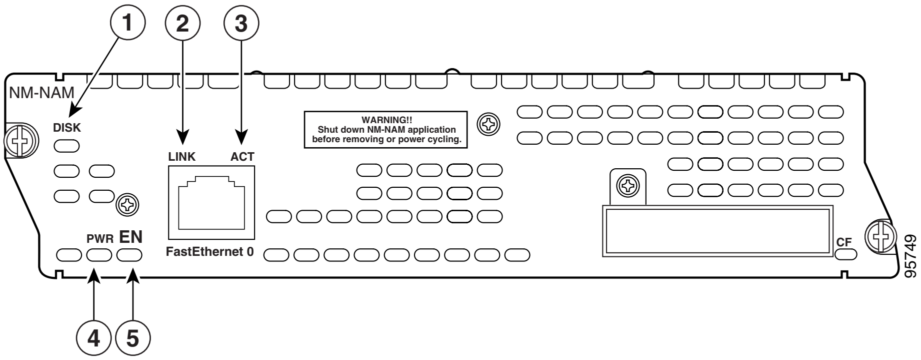

1
2
3
NM-NAM
DISK
LINK
ACT
WARNING!!
Shut down NM-NAM application before removing or power cycling.
PWR
EN
FastEthernet 0
CF
95749
4
5

Figure 54 Callout	LED	Indicates
1	DISK	There is activity on the hard drive.
2	LINK	The Fast Ethernet connection is available to the network module.
3	ACT	There is activity on the Fast Ethernet connection.
4	PWR	Power is available to the network module.
5	EN	The module has passed self-test and is available to the router.

NAM User Interfaces

The NAM has three user interfaces:

- Web GUI—The NAM Traffic Analyzer provides a browser-based GUI to configure and monitor the NAM.
- CLI—A NAM-specific command-line interface is used to configure NAM. It can be accessed through a NAM console session from the router or through Telnet or Secure Shell Protocol (SSH) over the network.
- SNMP—The NAM supports SNMPv1 and SNMPv2c access to the RMON MIBs. Note that the NAM Simple Network Management Protocol (SNMP) agent is separate from the SNMP agent in the router; the agents use different IP addresses and have independent communities.

NAM Network Interfaces

The NAM uses three interfaces for communication (see Figure 55):

- Analysis-Module Interface
- Internal NAM Interface
- External NAM Interface

Note The NM-NAM does not have an external console port. To access the NAM console, open a NAM console session from the router or use Telnet or SSH over the network. The lack of an external console port on the NM-NAM means that the initial boot configuration is possible only through the router.

Figure 55 NAM Network Interfaces

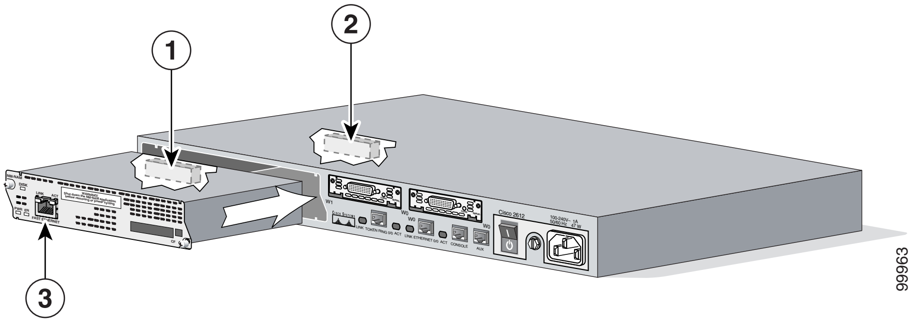


Figure 55 Callout	Interface	Location	Configure and Manage From
1	Internal NAM interface	NM-NAM internal	NAM CLI
2	Analysis-Module interface	Router internal	Cisco IOS CLI
3	External NAM interface	NM-NAM faceplate	NAM CLI

Analysis-Module Interface

The Analysis-Module interface is used to access the NAM console for the initial configuration. After configuring the NAM IP parameters, the Analysis-Module interface is typically used only during NAM software upgrades and while troubleshooting if the NAM Traffic Analyzer is inaccessible.

Visible only to the Cisco IOS software on the router, the Analysis-Module interface is an internal Fast Ethernet interface on the router that connects to the internal NAM interface. The Analysis-Module interface is connected to the router's Peripheral Component Interconnect (PCI) backplane, and all configuration and management of the Analysis-Module interface must be performed from the Cisco IOS CLI.

Internal NAM Interface

The internal NAM interface is used for monitoring traffic that passes through router interfaces. You can also select the internal NAM interface as the management interface for the NAM.

Visible only to the NAM software on the NM-NAM, the internal NAM interface is the Fast Ethernet interface on the NM-NAM that connects to the Analysis-Module interface on the router. The internal NAM interface is connected to the PCI bus on the NM-NAM, and all configuration and management of the internal NAM interface must be performed from the NAM software.

External NAM Interface

The external NAM interface can be used to monitor LAN traffic. You can also select the external NAM interface as the management interface for the NAM.

Visible only to the NAM software on the NM-NAM, the external NAM interface is the Fast Ethernet interface on the NM-NAM faceplate (see Figure 54 on page 574). The external NAM interface supports data requests and data transfers from outside sources, and it provides direct connectivity to the LAN through an RJ-45 connector. All configuration and management of the external NAM interface must be performed from the NAM software.

NM-NAM Operating Topologies and IP Address Assignments

This section includes the following topics:

- Management Traffic—Choose One of the NM-NAM Interfaces, page 576
- Monitored Traffic—Use One or Both of the NM-NAM Interfaces, page 577
- Sample Operating Topologies, page 578

Management Traffic—Choose One of the NM-NAM Interfaces

Select either the internal or external NAM interface to handle management traffic such as IP, HTTP, SNMP, Telnet, and SSH. You cannot send management traffic through both NAM interfaces at the same time.

How you assign IP addresses on the NAM network interfaces depends on which NAM interface, internal or external, you use for management traffic. See the following sections:

- Internal NAM Interface for Management Traffic—How to Assign IP Addresses, page 576
- External NAM Interface for Management Traffic—How to Assign IP Addresses, page 577

Internal NAM Interface for Management Traffic—How to Assign IP Addresses

If you select the internal NAM interface to handle management traffic:

- For the Analysis-Module interface (in Cisco IOS CLI), assign an IP address from a routable subnet. To conserve IP address space, you can configure the Analysis-Module as an IP unnumbered interface and borrow the IP address of another router interface, such as a Fast Ethernet or loopback interface. The borrowed IP address must come from a routable subnet.
- For the NAM system (in NAM CLI), assign an IP address from the same subnet that is assigned to the Analysis-Module interface.

External NAM Interface for Management Traffic—How to Assign IP Addresses

If you select the external NAM interface to handle management traffic:

- For the Analysis-Module interface (in Cisco IOS CLI), we recommend that you use the IP unnumbered interface configuration to borrow the IP address of another router interface. The subnet does not need to be routable.
- For the NAM system (in NAM CLI), assign an IP address from the subnet that is connected to the external NAM interface.

Monitored Traffic—Use One or Both of the NM-NAM Interfaces

You can use either or both the internal and external NAM interfaces for monitoring traffic:

- Internal NAM Interface—Monitor LAN and WAN Traffic, page 577
- External NAM Interface—Monitor LAN Traffic, page 577

The same interface can be used for both management traffic and monitored traffic simultaneously.

Internal NAM Interface—Monitor LAN and WAN Traffic

When you monitor traffic through the internal NAM interface, you must enable NAM packet monitoring on each router interface that you want to monitor. NAM packet monitoring uses Cisco Express Forwarding (CEF) to send a copy of each packet that is received or sent out of the router interface to the NAM.

Note Some restrictions apply when monitoring traffic through the internal NAM interface. See the "Traffic Monitoring Restrictions for the Internal NAM Interface" section on page 572.

Monitoring traffic through the internal NAM interface enables the NAM to see any encrypted traffic after it has already been decrypted by the router.

Note Traffic sent through the internal NAM interface—and the router's Analysis-Module interface—uses router resources such as CPU, SDRAM bandwidth, and backplane PCI bandwidth. Therefore, we recommend that you use the internal NAM interface to monitor WAN interfaces, and use the external NAM interface to monitor LAN interfaces.

External NAM Interface—Monitor LAN Traffic

Monitoring traffic through the external NAM interface does not impact router resources. Therefore, we recommend that you use the external NAM interface to monitor LAN traffic.

To monitor ports on Ethernet switching cards or modules (NM-16ESW-*x*, NMD-36ESW-*x*, HWIC-4ESW, or HWIC-D-9ESW), configure a Switched Port Analyzer (SPAN) session whose destination is the Ethernet switch port that connects to the external NAM interface. For more information about configuring SPAN for these cards and modules, refer to the following documents:

- *16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series*, Cisco IOS feature module
- *Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch Interface Cards*, Cisco IOS feature module

Sample Operating Topologies

In each of the following topologies, the router's LAN interface is monitored through the external NAM interface, and the router's WAN interface is monitored through the internal NAM interface:

- NAM Management Interface Is Internal and Analysis-Module Interface Is Assigned an IP Address, page 578
- NAM Management Interface Is Internal and Analysis-Module Interface Is IP Unnumbered, page 579
- NAM Management Interface Is External and Analysis-Module Interface Is IP Unnumbered, page 580

To see sample configurations for the following topologies, see the "Configuration Examples for the Network Analysis Module (NM-NAM)" section on page 617.

NAM Management Interface Is Internal and Analysis-Module Interface Is Assigned an IP Address

Figure 56 shows a sample topology, in which:

- The internal NAM interface is used for management traffic.
- IP addresses from the same routable subnet are assigned to the Analysis-Module interface and the NAM system.

Figure 56 Sample Topology: NAM Management Interface Is Internal and Analysis-Module Interface Is Assigned an IP Address

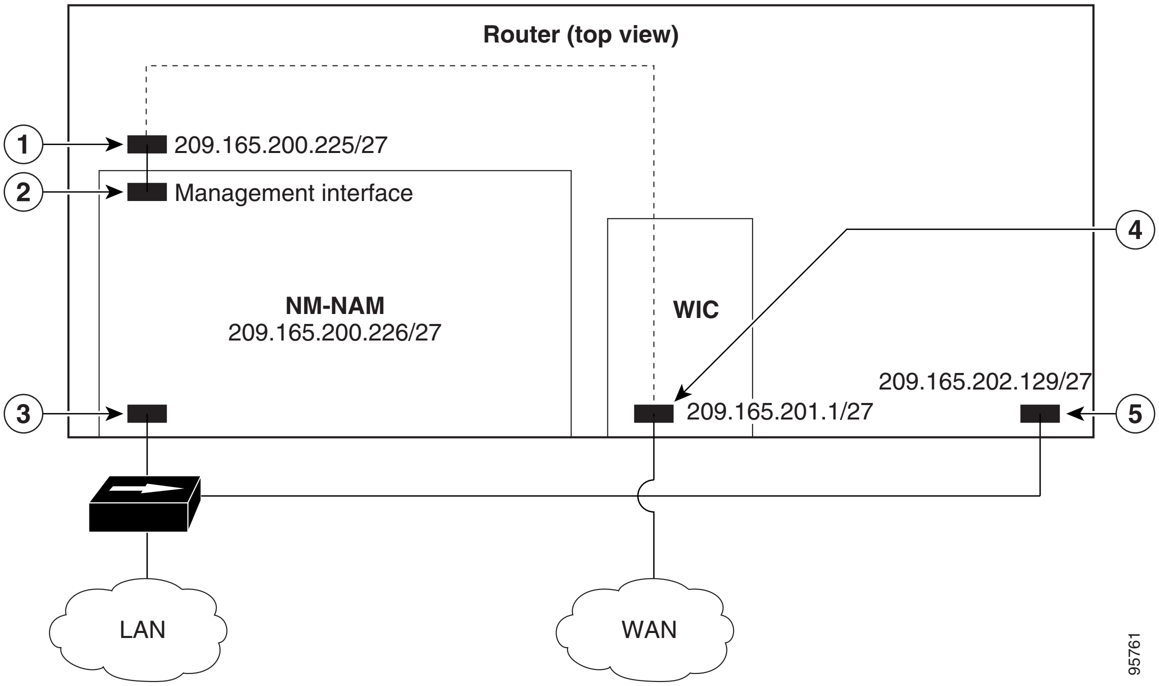


Figure 56 Callout	Interface	Location
1	Analysis-Module interface	Router internal
2	Internal NAM interface (**management**)	NM-NAM internal

Figure 56 Callout	Interface	Location
3	External NAM interface	NM-NAM faceplate
4	Serial interface	WAN interface card (WIC)
5	Fast Ethernet interface	Router rear panel

NAM Management Interface Is Internal and Analysis-Module Interface Is IP Unnumbered

Figure 57 shows a sample topology, in which:

- The internal NAM interface is used for management traffic.
- IP addresses from the same routable subnet are assigned to the Analysis-Module interface and the NAM system.
- To conserve IP address space, the Analysis-Module interface is configured as IP unnumbered to borrow the IP address of the Fast Ethernet interface.

Figure 57 Sample Topology: NAM Management Interface Is Internal and Analysis-Module Interface Is IP Unnumbered

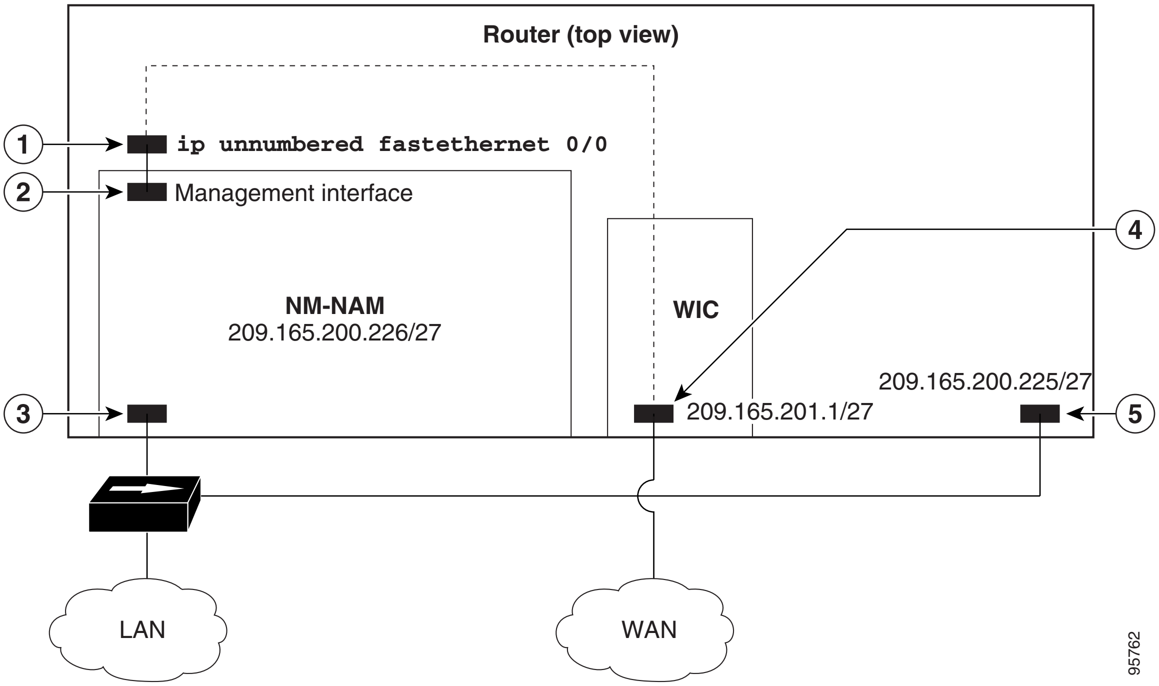


Figure 57 Callout	Interface	Location
1	Analysis-Module interface	Router internal
2	Internal NAM interface (**management**)	NM-NAM internal
3	External NAM interface	NM-NAM faceplate

Figure 57 Callout	Interface	Location
4	Serial interface	WAN interface card (WIC)
5	Fast Ethernet interface	Router rear panel

NAM Management Interface Is External and Analysis-Module Interface Is IP Unnumbered

Figure 58 shows a sample topology where:

- The external NAM interface is used for management traffic.
- The Analysis-Module interface is configured as IP unnumbered to borrow an IP address from the loopback interface.
- The borrowed loopback interface IP address is not routable.
- The NAM system is configured with an IP address from the LAN subnet that is connected to the external NAM interface.

Figure 58 Sample Topology: NAM Management Interface Is External and Analysis-Module Interface Is IP Unnumbered

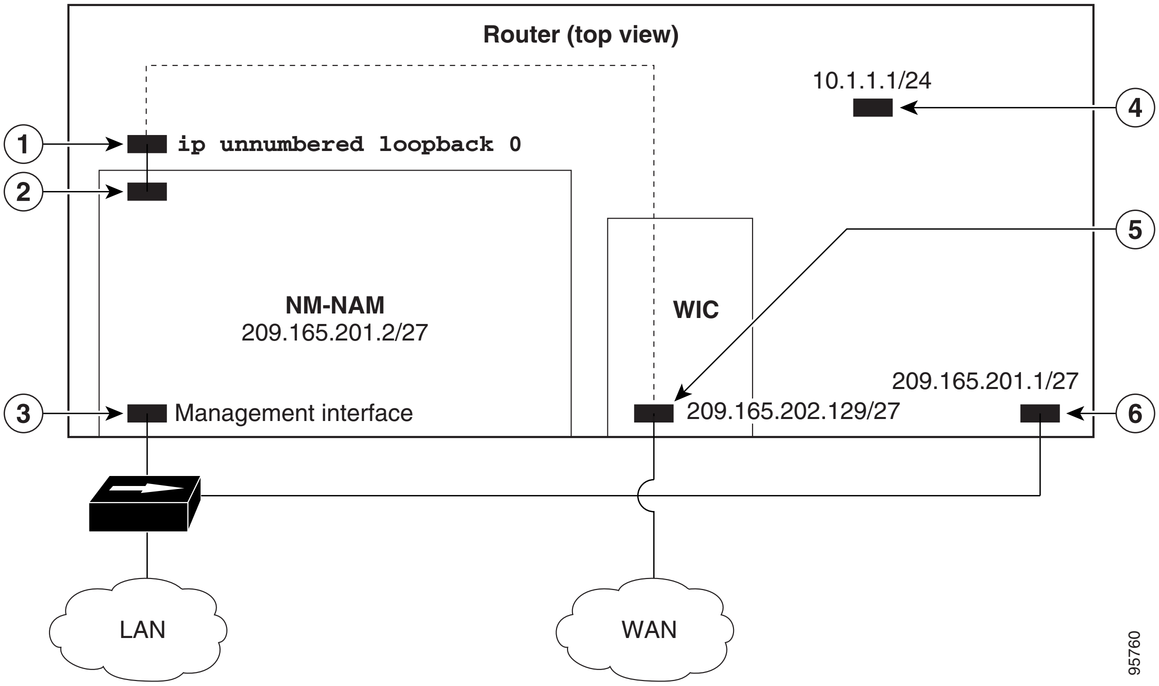


Figure 58 Callout	Interface	Location
1	Analysis-Module interface	Router internal
2	Internal NAM interface	NM-NAM internal
3	External NAM interface (**management**)	NM-NAM faceplate
4	Loopback interface	Router internal

Figure 58 Callout	Interface	Location
5	Serial interface	WAN interface card (WIC)
6	Fast Ethernet interface	Router rear panel

NAM CLI

This section includes the following topics:

- NAM CLI Access
- NAM CLI Prompt
- Basic NAM CLI Commands
- NAM CLI Context-Sensitive Help

NAM CLI Access

There are three ways to access the NAM CLI:

- Open a NAM console session from the router in which the NM-NAM is installed—See the "Opening and Closing a NAM Console Session from the Router" section on page 588.
- Telnet—See the "Opening and Closing a Telnet or SSH Session to the NAM" section on page 608.
- SSH—See the "Opening and Closing a Telnet or SSH Session to the NAM" section on page 608.

Until you properly configure the NAM IP parameters, the only way to access the NAM CLI is by opening a NAM console session from the router.

NAM CLI Prompt

The NAM CLI prompt is `root@`*`nam-system-hostname`*`#`. For example, if the NAM system hostname is configured as "nam1," then the NAM CLI prompt appears as `root@nam1#`.

If the NAM system hostname has not yet been configured, the NAM CLI prompt is `root@localhost#`.

Basic NAM CLI Commands

Table 33 briefly describes the basic NAM CLI commands that are used for initial configuration and maintenance of the NM-NAM. For a complete description of all NAM CLI commands, refer to the *Network Analysis Module Command Reference* for your NAM software release.

Note Although NAM CLI commands appear similar to Cisco IOS commands, the commands described in Table 33 operate in the NAM CLI only.

Table 33 Basic NAM CLI Commands

NAM CLI Command	Purpose
exsession on	Enables outside logins (Telnet).
exsession on ssh	Enables outside logins (SSH).

Table 33 Basic NAM CLI Commands (continued)

NAM CLI Command	Purpose
ip address	Sets the system IP address.
ip broadcast	Sets the system broadcast address.
ip domain	Sets the system domain name.
ip gateway	Sets the system default gateway address.
ip host	Sets the system hostname.
ip http secure server enable	Enables the secure HTTP server.
ip http server enable	Enables the HTTP server.
ip interface external	Selects the external NAM interface for management traffic.
ip interface internal	Selects the internal NAM interface for management traffic.
ip nameserver	Sets the system name server address.
password root	Sets a new password to access the root (read/write) level of NAM.
patch	Downloads and installs a software patch.
ping	Checks connectivity to a network device.
show ip	Displays the NAM IP parameters.

NAM CLI Context-Sensitive Help

Table 34 shows how to use the NAM CLI context-sensitive help.

Table 34 NAM CLI Context-Sensitive Help Commands

NAM CLI Command	Purpose

`(prompt)# ?`
or
`(prompt)# help`
	Displays a list of commands available for the command mode.

`(prompt)# abbreviated-command-entry<Tab>`	Lists commands in the current mode that begin with a particular character string.
`(prompt)# command ?`	Lists the available syntax options (arguments and keywords) for the command.
`(prompt)# command keyword ?`	Lists the next available syntax option for the command.

How to Configure and Manage the Network Analysis Module (NM-NAM)

This section contains the following procedures:

- Configuring the Analysis-Module Interface on the Router, page 583 (required)
- Disabling AAA Login Authentication on the NAM Console Line, page 586 (optional)
- Opening and Closing a NAM Console Session from the Router, page 588 (required for initial configuration)
- Configuring the NM-NAM, page 591 (required for initial configuration)
- Configuring a Static Route to the NAM Through the Analysis-Module Interface, page 595 (required for using the internal NAM interface for management traffic)
- Enabling NAM Packet Monitoring, page 597 (required for monitoring traffic through the internal NAM interface)
- Enabling and Accessing the NAM Traffic Analyzer, page 599 (required)
- Changing the NAM Root Password, page 602 (optional)
- Resetting the NAM Root Password to the Default Value, page 604 (optional)
- Opening and Closing a Telnet or SSH Session to the NAM, page 608 (optional)
- Upgrading the NAM Software, page 611 (optional)

Configuring the Analysis-Module Interface on the Router

This section describes how to configure the Analysis-Module interface on the router. For general information on the Analysis-Module interface, see the "Analysis-Module Interface" section on page 575.

For information on assigning the IP address of the Analysis-Module interface, see the "NM-NAM Operating Topologies and IP Address Assignments" section on page 576.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **interface analysis-module** *slot*/**0**
6. **ip unnumbered** *interface number*
   or
   ip address *ip-address mask*
7. **no shutdown**
8. **end**
9. **show ip interface brief**
   or
   show running-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface loopback 0`	(Optional) Configures an interface, and enters interface configuration mode. • Perform this step if you plan to configure the Analysis-Module interface as an IP unnumbered interface. • This step configures the router interface (such as a loopback or Fast Ethernet interface) whose IP address you plan to borrow for the IP unnumbered Analysis-Module interface.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.20.30.40 255.255.255.0`	(Optional) Sets an IP address and mask for the interface. • Perform this step if you plan to configure the Analysis-Module interface as an IP unnumbered interface. • If you plan to use the internal NAM interface for management traffic, this IP address must come from a routable subnet.
Step 5	**interface analysis-module** *slot*/**0** **Example:** `Router(config)# interface analysis-module 1/0`	Configures the Analysis-Module interface. • This is the Fast Ethernet interface on the router that is connected to the internal NM-NAM interface.

Step 6	**ip unnumbered** *interface number*
	or
	ip address *ip-address mask*
	Example:
	`Router(config-if)# ip unnumbered loopback 0`
	Example:
	`Router(config-if)# ip address 10.20.30.40 255.255.255.0`
		Configures the Analysis-Module interface as IP unnumbered and specifies the interface whose IP address is borrowed by the Analysis-Module interface.
		or
		Sets an IP address and mask on the Analysis-Module interface.
		• Use the **ip unnumbered** command if you performed Step 3 and Step 4.

	Command or Action	Purpose
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the Analysis-Module interface.

Step 8	**end**
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

Step 9	**show ip interface brief**
	or
	show running-config
	Example:
	`Router# show ip interface brief`
	Example:
	`Router# show running-config`
		Displays the IP addresses and summary status of the interfaces.
		or
		Displays the contents of the currently running configuration file.
		• Verify that you properly configured the Analysis-Module interface.
		• If you configured the Analysis-Module interface as IP unnumbered, then use the **show running-config** command to verify proper configuration of both the Analysis-Module interface and the interface whose IP address you borrowed for the Analysis-Module interface.

Tip To avoid losing your configuration at the next system reload or power cycle, save the running configuration to the startup configuration by entering the **copy run start** command in privileged EXEC mode.

Examples

This section provides the following examples:

- Configuring the Analysis-Module Interface—Routable Subnet: Example, page 585
- Configuring the Analysis-Module Interface—IP Unnumbered with Routable Subnet: Example, page 586
- Configuring the Analysis-Module Interface—IP Unnumbered with Subnet That Is Not Routable: Example, page 586
- Sample Output for the show ip interface brief Command, page 586

Configuring the Analysis-Module Interface—Routable Subnet: Example

In the following example, the Analysis-Module interface is configured with a routable IP address. The NM-NAM is installed in router slot 2.

```
!
interface Analysis-Module 2/0
 ip address 209.165.200.230 255.255.255.224
 no shutdown
```

Configuring the Analysis-Module Interface—IP Unnumbered with Routable Subnet: Example

In the following example, the Analysis-Module interface is IP unnumbered and borrows the IP address of the Fast Ethernet interface. The IP address is from a routable subnet, and the NM-NAM is installed in router slot 1.

```
!
interface FastEthernet 0/0
 ip address 209.165.202.129 255.255.255.224
 no shutdown
!
interface Analysis-Module 1/0
 ip unnumbered FastEthernet 0/0
 no shutdown
!
```

Configuring the Analysis-Module Interface—IP Unnumbered with Subnet That Is Not Routable: Example

In the following example, the Analysis-Module interface is IP unnumbered and borrows a loopback interface IP address that is not routable. The NM-NAM is installed in router slot 3.

```
!
interface loopback 0
 ip address 10.20.30.40 255.255.255.0
!
interface Analysis-Module 3/0
 ip unnumbered loopback 0
 no shutdown
!
```

Sample Output for the show ip interface brief Command

```
Router# show ip interface brief

Interface                  IP-Address      OK?   Method       Status         Protocol
FastEthernet0/0            172.20.105.213  YES   NVRAM        up             up
FastEthernet0/1            172.20.105.53   YES   NVRAM        up             up
Analysis-Module2/0         10.1.1.1        YES   manual       up             up
Router#
```

What to Do Next

If you configured authentication, authorization, and accounting (AAA) on your router, then proceed to the "Disabling AAA Login Authentication on the NAM Console Line" section on page 586.

Otherwise, proceed to the "Opening and Closing a NAM Console Session from the Router" section on page 588.

Disabling AAA Login Authentication on the NAM Console Line

If you configured authentication, authorization, and accounting (AAA) on your router, then you may have to log in twice to open a NAM console session from the router: first with your AAA username and password, and second with the NAM login and password.

If you do not want to log in twice to open a NAM console session from the router, then disable AAA login authentication on the router's NAM console line by performing the steps in this section.

Note, however, that if your router contains both the NM-NAM and the NM-CIDS, the Cisco intrusion detection system network module, then AAA can be a useful tool for centrally controlling access to both network modules. For information about AAA, refer to the *Cisco IOS Security Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication login** *list-name* **none**
4. **line** *number*
5. **login authentication** *list-name*
6. **end**
7. **show running-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`aaa authentication login`** *`list-name`* **`none`**
	Example:
	`Router(config)# aaa authentication login nam none`
		Creates a local authentication list.
		• The **none** keyword specifies no authentication for this list.

Step 4	**`line`** *`number`*
	Example:
	`Router(config)# line 33`
		Enters line configuration mode for the line to which you want to apply the authentication list.
		• The *number* value is determined by the slot number in which the NM-NAM is installed:
		number = (32 x *slot*) + 1

Step 5	**`login authentication`** *`list-name`*
	Example:
	`Router(config-line)# login authentication nam`
		Applies the authentication list to the line.
		• Specify the list name that you configured in Step 3.

Step 6	**`end`**
	Example:
	`Router(config-line)# end`
	`Router#`
		Returns to privileged EXEC mode.

Step 7	**`show running-config`**
	Example:
	`Router# show running-config`
		Displays the contents of the currently running configuration file.
		• Verify that you configured the local authentication list and applied it to the line associated with the NM-NAM.

What to Do Next

Proceed to the "Opening and Closing a NAM Console Session from the Router" section on page 588.

Opening and Closing a NAM Console Session from the Router

This section describes how to open and close a NAM console session from the router.

SUMMARY STEPS

1. **enable**
2. **service-module analysis-module** *slot*/**0 session**
3. Press **Return**.
   or
   If a username prompt appears, then log in with your AAA username and password.
4. At the login prompt, enter **root**.
5. At the password prompt, enter your password.
   or
   If you have not changed the password from the factory-set default, enter **root** as the root password.
6. Perform the tasks that you need to perform in the NAM CLI. When you want to end the NAM console session and return to the Cisco IOS CLI, complete Step 7 through Step 10.
7. **exit**
8. Hold **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.
9. **disconnect**
10. Press **Enter**.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`service-module analysis-module`** *`slot`*`/`**`0 session`**
	Example:
	`Router# service-module analysis-module 1/0 session`
	Example:
	`Router# service-module analysis-module 1/0 session clear`
	`[confirm]`
	` [OK]`
	`Router# service-module analysis-module 1/0 session`
		Establishes a console session with the NAM.
		• If you cannot open a NAM console session, make sure that the NAM console line is clear by first entering the **service-module analysis-module** *slot*/**0 session clear** command in privileged EXEC mode.

	Command or Action	Purpose

Step 3	Press **Return**.
	or
	If a username prompt appears, then log in with your AAA username and password.
	Example:
	`Trying 10.1.1.1, 2065 ... Open`
	`<Press Return>`
	
	`Cisco Network Analysis Module (NM-NAM)`
	
	`nam1.cisco.com login:`
	Example:
	`Trying 10.1.1.1, 2065... Open`
	`User Access Verification`
	
	`Username: myaaausername`
	`Password: <myaaapassword>`
	`Cisco Network Analysis Module (NM-NAM)`
	
	`nam1.cisco.com login:`
		Activates the NAM console line.
		or
		Completes AAA login authentication and activates the NAM console line.
		• If AAA is configured on your router and you do not want to log in twice to access the NAM console, then complete the steps in the "Disabling AAA Login Authentication on the NAM Console Line" section on page 586.

Step 4	At the login prompt, enter **root**. **Example:** `login: root`	Accesses the root (read/write) level of NAM.
Step 5	At the password prompt, enter your password. or If you have not changed the password from the factory-set default, enter **root** as the root password. **Example:** `Password: <root>`	—
Step 6	Perform the tasks that you need to perform in the NAM CLI. When you want to end the NAM console session and return to the Cisco IOS CLI, complete Step 7 through Step 10.	For initial configuration tasks, see the "Configuring the NM-NAM" section on page 591. For help using NAM CLI commands, see the "NAM CLI Context-Sensitive Help" section on page 582.

Step 7	**`exit`**
	Example:
	`root@localhost(sub-custom-filter-capture)# exit`
	`root@localhost# exit`
	
	`login:`
		Logs out of the NAM system or leaves a subcommand mode.
		• If you are in a subcommand mode, continue to enter the **exit** command until you see the NAM login prompt.

	Command or Action	Purpose

Step 8	Hold **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.
	Example:
	`login: <suspend keystroke>`
	`Router#`
		Suspends and closes the Telnet session.

Step 9	**`disconnect`**
	Example:
	`Router# disconnect`
		Disconnects a line.

Step 10	Press **Enter**.
	Example:
	`Closing connection to 10.20.30.40 [confirm]`
	`<Enter>`
		Confirms that you want to disconnect the line.

Examples

This section provides the following examples:

- Opening and Closing a NAM Console Session When AAA Authentication Is Not Configured or Is Disabled on the NAM Console Line: Example, page 590
- Opening and Closing a NAM Console Session When AAA Authentication Is Configured and Enabled on the NAM Console Line: Example, page 591

Opening and Closing a NAM Console Session When AAA Authentication Is Not Configured or Is Disabled on the NAM Console Line: Example

In the following example, a NAM console session is opened and closed from the router. The NM-NAM is installed in router slot 2.

```
Router# service-module analysis-module 2/0 session
Trying 10.1.1.1, 2065 ... Open


Cisco Network Analysis Module (NM-NAM)

nam1.cisco.com login: root
Password: <password>
Terminal type: vt100

Cisco Network Analysis Module (NM-NAM) Console, 3.2
Copyright (c) 1999-2003 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@nam1.cisco.com#
root@nam1.cisco.com# exit


Cisco Network Analysis Module (NM-NAM)

nam1.cisco.com login: <suspend keystroke>
Router# disconnect
Closing connection to 10.1.1.1 [confirm] <Enter>
Deleting login session
```

Opening and Closing a NAM Console Session When AAA Authentication Is Configured and Enabled on the NAM Console Line: Example

In the following example, a NAM console session is opened and closed from the router. The NM-NAM is installed in router slot 2.

```
Router# service-module analysis-module 2/0 session
Trying 10.1.1.1, 2065 ... Open
User Access Verification

Username: myaaausername
Password: <myaaapassword>
Cisco Network Analysis Module (NM-NAM)

nam1.cisco.com login: root
Password: <nampassword>
Terminal type: vt100

Cisco Network Analysis Module (NM-NAM) Console, 3.2
Copyright (c) 1999-2003 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@nam1.cisco.com#
root@nam1.cisco.com# exit



Cisco Network Analysis Module (NM-NAM)

nam1.cisco.com login: <suspend keystroke>
Router# disconnect
Closing connection to 10.1.1.1 [confirm] <Enter>
Deleting login session
```

Troubleshooting Tips

Make sure that the NAM console line is clear by entering the **service-module analysis-module** *slot*/**0 session clear** command in privileged EXEC mode.

What to Do Next

Proceed to the "Configuring the NM-NAM" section.

Configuring the NM-NAM

This section describes how to configure the NM-NAM to establish network connectivity and configure IP parameters. This task must be performed from the NAM CLI. For more advanced NAM configuration, use the NAM Traffic Analyzer (web GUI) or refer to the *Network Analysis Module Command Reference* for your NAM software release.

For information on assigning IP addresses, see the "NM-NAM Operating Topologies and IP Address Assignments" section on page 576.

Prerequisites

Before performing this task, access the NAM console by performing Step 1 through Step 5 in the "Opening and Closing a NAM Console Session from the Router" section on page 588.

SUMMARY STEPS

1. **ip interface** {**internal** | **external**}
2. **ip address** *ip-address subnet-mask*
3. **ip broadcast** *broadcast-address*
4. **ip gateway** *ip-address*
5. **exsession on**
   or
   exsession on ssh
6. **ip domain** *name*
7. **ip host** *name*
8. **ip nameserver** *ip-address* [*ip-address*][*ip-address*]
9. **ping** {*host* | *ip-address*}
10. **show ip**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**ip interface** {**internal** | **external**}
	Example:
	`root@localhost# ip interface internal`
	Example:
	`root@localhost# ip interface external`
		Specifies which NAM interface will handle management traffic.

Step 2	**ip address** *ip-address subnet-mask* **Example:** `root@localhost# ip address 172.20.104.126 255.255.255.248`	Configures the NAM system IP address. • For information on assigning the IP address, see the "Management Traffic—Choose One of the NM-NAM Interfaces" section on page 576.
Step 3	**ip broadcast** *broadcast-address* **Example:** `root@localhost# ip broadcast 10.255.255.255`	(Optional) Configures the NAM system broadcast address.
Step 4	**ip gateway** *ip-address* **Example:** `root@localhost# ip gateway 172.20.104.125`	Configures the NAM system default gateway address.

	Command or Action	Purpose

Step 5	**`exsession on`**
	or
	`exsession on ssh`
	Example:
	`root@localhost# exsession on`
	Example:
	`root@localhost# exsession on ssh`
		(Optional) Enables outside logins.
		• **exsession on** enables Telnet access.
		• **exsession on ssh** enables SSH access.
		Note The NAM software K9 crypto patch is required to configure the **ssh** option. You can download the patch from Cisco.com.

Step 6	**`ip domain`** *`name`*
	Example:
	`root@localhost# ip domain cisco.com`
		(Optional) Sets the NAM system domain name.

Step 7	**`ip host`** *`name`*
	Example:
	`root@localhost# ip host nam1`
		(Optional) Sets the NAM system hostname.

Step 8	**`ip nameserver`** *`ip-address`* `[`*`ip-address`*`][`*`ip-address`*`]`
	Example:
	`root@nam1# ip nameserver 209.165.201.1`
		(Optional) Sets one or more NAM system name servers.
		• We recommend that you configure a name server for the NAM system to resolve Domain Name System (DNS) requests.

Step 9	**`ping`** `{`*`host`* `|` *`ip-address`*`}`
	Example:
	`root@nam1# ping 10.20.30.40`
		Checks connectivity to a network device.
		• Verify connectivity to the router or another known host.

Step 10	**`show ip`**
	Example:
	`root@nam1# show ip`
		Displays the NAM IP parameters.
		• Verify that you properly configured the NM-NAM.

Examples

This section provides the following examples:

- Configuring the NM-NAM: Example, page 594
- Checking Network Connectivity with Ping: Example, page 594
- Sample Output for the show ip NAM CLI Command, page 594

Configuring the NM-NAM: Example

In the following example, the external NAM interface is used for management traffic. The HTTP server and Telnet access are enabled. The resulting NAM CLI prompt is `root@nam1.cisco.com#`.

```
!
ip address 172.20.105.215 255.255.255.192
!
ip host "nam1"
!
ip domain "cisco.com"
!
ip gateway 172.20.105.210
!
ip broadcast 10.255.255.255
!
ip nameserver 209.165.201.29
!
ip interface external
!
ip http server enable
!
exsession on
!
```

Checking Network Connectivity with Ping: Example

```
root@nam1.cisco.com# ping 172.20.105.213

PING 172.20.105.213 (172.20.105.213) from 172.20.105.215 : 56(84) bytes of data.
64 bytes from 172.20.105.213: icmp_seq=0 ttl=255 time=353 usec
64 bytes from 172.20.105.213: icmp_seq=1 ttl=255 time=289 usec
64 bytes from 172.20.105.213: icmp_seq=2 ttl=255 time=284 usec
64 bytes from 172.20.105.213: icmp_seq=3 ttl=255 time=283 usec
64 bytes from 172.20.105.213: icmp_seq=4 ttl=255 time=297 usec

--- 172.20.105.213 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.283/0.301/0.353/0.028 ms
root@nam1.cisco.com#
```

Sample Output for the show ip NAM CLI Command

```
root@nam1.cisco.com# show ip

IP address:            172.20.105.215
Subnet mask:           255.255.255.192
IP Broadcast:          10.255.255.255
IP Interface:          External
DNS Name:              nam1.cisco.com
Default Gateway:       172.20.105.210
Nameserver(s):         209.165.201.29
HTTP server:           Enabled
HTTP secure server:    Disabled
HTTP port:             80
HTTP secure port:      443
TACACS+ configured:    No
Telnet:                Enabled
SSH:                   Disabled
root@nam1.cisco.com#
```

What to Do Next

If you selected the internal NAM interface to handle management traffic in Step 1, then proceed to the "Configuring a Static Route to the NAM Through the Analysis-Module Interface" section on page 595.

If you plan to monitor traffic through the internal NAM interface, then proceed to the "Enabling NAM Packet Monitoring" section on page 597.

If you do not plan to monitor traffic through the internal NAM interface, then proceed to the "Enabling and Accessing the NAM Traffic Analyzer" section on page 599.

Configuring a Static Route to the NAM Through the Analysis-Module Interface

This section describes how to ensure that the router can route packets to the NAM by configuring a static route through the Analysis-Module interface.

If you select the internal NAM interface to handle management traffic, then configuring a static route to the NAM through the Analysis-Module interface is:

- Required when the Analysis-Module interface is IP unnumbered.
- Recommended when the Analysis-Module interface is assigned a unique IP address.

If you select the external NAM interface to handle management traffic, then you do not need to perform this task. Proceed to the "What to Do Next" section on page 597.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *nam-ip-address mask* **analysis-module** *slot/unit*
4. **end**
5. **ping** {*nam-ip-address* | *nam-hostname*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip route** *nam-ip-address mask* **analysis-module** *slot***/***unit* **Example:** `Router(config)# ip route 172.20.105.215 255.255.255.192 analysis-module 1/0`	Establishes a static route to the NAM.

Step 4	**end**
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

Step 5	**ping** {*nam-ip-address* | *nam-hostname*}
	Example:
	`Router# ping 172.20.105.215`
		Verifies network connectivity to the NAM.

Examples

This section provides the following examples:

- Configuring a Static Route to the NAM Through the Analysis-Module Interface: Example, page 596
- Verifying Network Connectivity with Ping: Example, page 596

Configuring a Static Route to the NAM Through the Analysis-Module Interface: Example

In the following example, a static route is configured to the NAM whose system IP address is 172.20.105.215. The NM-NAM is installed in router slot 1.

```
!
ip route 172.20.105.215 255.255.255.192 analysis-module 1/0
!
interface FastEthernet 0/0
 ip address 209.165.202.129 255.255.255.224
 no shutdown
!
interface Analysis-Module 1/0
 ip unnumbered FastEthernet 0/0
 no shutdown
!
```

Verifying Network Connectivity with Ping: Example

In the following example, entering the **ping** command verifies network connectivity to the NAM with IP address 172.20.105.215.

```
Router# ping 172.20.105.215

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.105.215, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#
```

What to Do Next

If you plan to monitor traffic through the internal NAM interface, then proceed to the "Enabling NAM Packet Monitoring" section on page 597.

If you do not plan to monitor traffic through the internal NAM interface, then proceed to the "Enabling and Accessing the NAM Traffic Analyzer" section on page 599.

Enabling NAM Packet Monitoring

This section describes how to enable NAM packet monitoring on router interfaces that you want to monitor through the internal NAM interface.

When you enable NAM packet monitoring on an interface, CEF sends an extra copy of each IP packet that is received or sent out on that interface to the NAM through the Analysis-Module interface on the router and the internal NAM interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **interface** *type slot/port*
or
interface *type slot/wic-slot/port*
5. **analysis-module monitoring**
6. Repeat Step 4 and Step 5 for each interface that you want the NAM to monitor.
7. **end**
8. **show running-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ip cef`
	Example:
	`Router(config)# ip cef`
		Enables the CEF switching path.

	Command or Action	Purpose
Step 4	**interface** *type slot/port* or **interface** *type slot/wic-slot/port* **Example:** `Router(config)# interface serial 0/0`	Selects an interface for configuration.
Step 5	**analysis-module monitoring** **Example:** `Router(config-if)# analysis-module monitoring`	Enables NAM packet monitoring on the interface.
Step 6	Repeat Step 4 and Step 5 for each interface that you want the NAM to monitor through the internal NAM interface.	—

Step 7	**end**
	Example:
	`Router(config-if)# end`
	`Router#`
		Returns to privileged EXEC mode.

Step 8	**show running-config** **Example:** `Router# show running-config`	Displays the contents of the currently running configuration file. • Verify that you enabled the CEF switching path and enabled packet monitoring on the correct interfaces.

Example

This section provides the following example:

- Enabling NAM Packet Monitoring: Example, page 598

Enabling NAM Packet Monitoring: Example

In the following example, NAM packet monitoring is enabled on the serial interfaces:

```
interface Serial 0/0
 ip address 172.20.105.213 255.255.255.240
 ip route-cache flow
 speed auto
 full-duplex
 analysis-module monitoring
 no mop enabled
!
interface Serial 0/1
 ip address 172.20.105.53 255.255.255.252
 ip route-cache flow
 duplex auto
 speed auto
 analysis-module monitoring
!
interface Analysis-Module 2/0
 ip address 10.1.1.1 255.255.255.0
 hold-queue 60 out
!
```

What to Do Next

Proceed to the "Enabling and Accessing the NAM Traffic Analyzer" section on page 599.

Enabling and Accessing the NAM Traffic Analyzer

This section describes how to enable and access the NAM Traffic Analyzer (web GUI).

Prerequisites

- Make sure that your web browser supports your NAM software release. For a list of supported browsers, refer to the NAM software release notes.
- If you plan to use the HTTP secure server (HTTPs), then you must first download and install the NAM software K9 crypto patch. Until you install the patch, the **ip http secure** commands are disabled. You can download the NAM software K9 crypto patch from Cisco.com.

Restrictions

You can use the HTTP server or the HTTP secure server, but you cannot use both simultaneously.

SUMMARY STEPS

1. Open a NAM console session from the router. See the "Opening and Closing a NAM Console Session from the Router" section on page 588.
   or
   Open a Telnet or SSH session to the NAM. See the "Opening and Closing a Telnet or SSH Session to the NAM" section on page 608.
2. **ip http server enable**
   or
   ip http secure server enable
3. Enter a web username.
   or
   Press **Return** to enter the default web username "admin".
4. Enter a password.
5. Enter the password again.
6. On your PC, open a web browser.
7. In the web browser, enter the NAM system IP address or hostname as the URL.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Open a NAM console session from the router. See the "Opening and Closing a NAM Console Session from the Router" section on page 588. or Open a Telnet or SSH session to the NAM. See the "Opening and Closing a Telnet or SSH Session to the NAM" section on page 608.	Accesses the NAM CLI.

Step 2	`ip http server enable`
	or
	`ip http secure server enable`
	Example:
	`root@localhost# ip http server enable`
	Example:
	`root@localhost# ip http secure server enable`
		Enables the HTTP server.
		or
		Enables the HTTP secure server (HTTPs).

Step 3	Enter a web username.
	or
	Press **Return** to enter the default web username "admin".
	Example:
	`Please enter a web administrator user name [admin]: joeadmin`
	Example:
	`Please enter a web administrator user name [admin]: <cr>`
		Configures a web username.
		• The NAM requires at least one web username and password configuration.
		• If NAM does not prompt you for a web username and password, then at least one web username and password combination was previously configured.

Step 4	Enter a password. **Example:** `New password: <adminpswd>`	Configures a password for the web username.
Step 5	Enter the password again. **Example:** `Confirm password: <adminpswd>`	Confirms the password for the web username.

	Command or Action	Purpose
Step 6	On your PC, open a web browser.	—

Step 7	In the web browser, enter the NAM system IP address or hostname as the URL.
	Example:
	`http://172.20.105.215/`
	Example:
	`https://172.20.105.215/`
	Example:
	`http://nam1/`
		Opens the NAM Traffic Analyzer in your web browser.
		• You are automatically redirected to the NAM Traffic Analyzer login page.

Examples

This section provides the following examples:

- Enabling the NAM Traffic Analyzer: Example, page 601
- Accessing the NAM Traffic Analyzer: Example, page 601

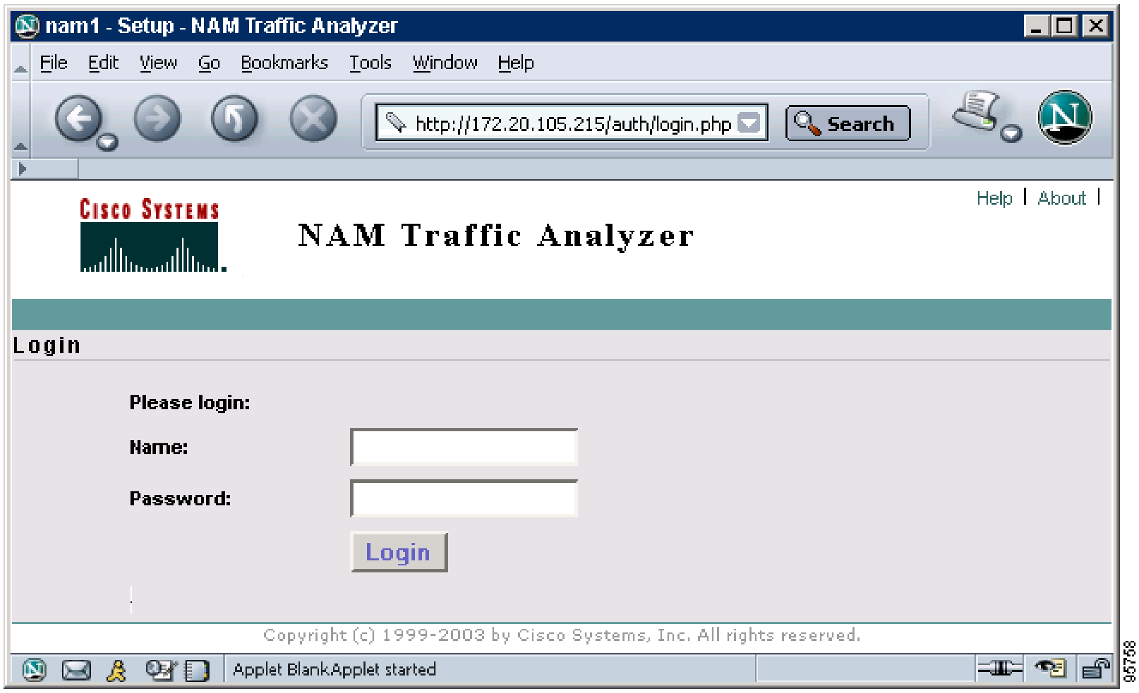
Enabling the NAM Traffic Analyzer: Example

```
root@nam1# ip http server enable
Enabling HTTP server...

No web users are configured.
Please enter a web administrator user name [admin]: <cr>
New password: <pswd>
Confirm password: <pswd>

User admin added.
Successfully enabled HTTP server.
root@nam1#
```

Accessing the NAM Traffic Analyzer: Example

Figure 59 shows the NAM Traffic Analyzer login page that appears when you enter the NAM system IP address or hostname as the URL in a web browser.

Figure 59 Sample NAM Traffic Analyzer Login Page


nam1 - Setup - NAM Traffic Analyzer
File Edit View Go Bookmarks Tools Window Help
http://172.20.105.215/auth/login.php
Search
Help | About |
Cisco Systems
NAM Traffic Analyzer
Login
Please login:
Name:
Password:
Login
Copyright (c) 1999-2003 by Cisco Systems, Inc. All rights reserved.
Applet BlankApplet started
95758

What to Do Next

For information on the NAM Traffic Analyzer, refer to the *User Guide for the Network Analysis Module Traffic Analyzer* for your NAM software release. This document is available on Cisco.com and as online help within the NAM Traffic Analyzer application.

Changing the NAM Root Password

This section describes how to set a new password to access the root (read/write) level of NAM, where you can enter NAM CLI commands. The factory-set default root password is "root".

Prerequisites

Before performing this task, access the NAM console by performing Step 1 through Step 5 in the "Opening and Closing a NAM Console Session from the Router" section on page 588.

SUMMARY STEPS

1. **password root**
2. Enter the new password.
3. Enter the new password again.
4. **exit**
5. At the login prompt, enter **root**.
6. At the password prompt, enter your password.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**password root** **Example:** `root@localhost.cisco.com# password root`	Starts the process of changing the NAM's root (read/write) level password.
Step 2	Enter the new password. **Example:** `New UNIX password: <password>`	Enters the new password.
Step 3	Enter the new password again. **Example:** `Retype new UNIX password: <password>`	Confirms the new password.
Step 4	**exit** **Example:** `root@localhost# exit`	Logs out of the NAM system.
Step 5	At the login prompt, enter **root**. **Example:** `login: root`	Accesses the root (read/write) level of NAM.
Step 6	At the password prompt, enter your password. **Example:** `Password: <password>`	Verifies that the new password is accepted.

Examples

This section provides the following examples:

- Changing the NAM Root Password: Example, page 603
- Verifying the NAM Root Password: Example, page 604

Changing the NAM Root Password: Example

```
root@nam1.cisco.com# password root
Changing password for user root
New UNIX password: <rtpswd>
Retype new UNIX password: <rtpswd>
passwd:all authentication tokens updated successfully
root@nam1.cisco.com#
root@nam1.cisco.com# exit
```

Verifying the NAM Root Password: Example

```
nam1.cisco.com login: root
Password: <rtpswd>
Terminal type: vt100

Cisco Network Analysis Module (NM-NAM) Console, 3.2
Copyright (c) 1999-2003 by cisco Systems, Inc.

root@nam1.cisco.com#
root@nam1.cisco.com# exit
```

Troubleshooting Tips

If you forget the NAM root password, see the "Resetting the NAM Root Password to the Default Value" section on page 604.

Resetting the NAM Root Password to the Default Value

This section describes how to reset the NAM root password to the default value of "root". Use this procedure when you cannot remember the NAM root password but need to access the NAM CLI.

Note This procedure requires that you reload the NAM software.

SUMMARY STEPS

1. **enable**
2. **service-module analysis-module** *slot*/**0 reload**
3. **y**
4. **service-module analysis-module** *slot*/**0 session**
5. When prompted, enter *** to change the boot configuration.
6. **boot flash**
7. When prompted to select from the helper menu, enter **6**.
8. When prompted to select from the helper menu, enter **r**.
9. **y**
10. Hold **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.
11. **disconnect**
12. Press **Enter**.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**service-module analysis-module** *slot*/**0 reload** **Example:** `Router# service-module analysis-module 1/0 reload`	Reloads the software on the NM-NAM.
Step 3	**y** **Example:** `Do you want to proceed with reload?[confirm] y`	Confirms that you want to proceed with the NAM software reload.

Step 4	**service-module analysis-module** *slot*/**0 session**
	Example:
	`Router# service-module analysis-module 1/0 session`
	Example:
	`Router# service-module analysis-module 1/0 session clear`
	`[confirm]`
	` [OK]`
	`Router# service-module analysis-module 1/0 session`
		Establishes a console session with the NAM.
		• Perform this step immediately after reloading the NAM software.
		• If you cannot open a NAM console session, make sure that the NAM console line is clear by first entering the **service-module analysis-module** *slot*/**0 session clear** command in privileged EXEC mode.

Step 5	When prompted, enter *** to change the boot configuration. **Example:** `Please enter '***' to change boot configuration: ***`	Interrupts the boot loader. • Enter *** immediately after the prompt appears. • If you do not enter *** in time to interrupt the boot loader, then the NAM login prompt eventually appears. Complete Step 10 through Step 12 to return to the Cisco IOS CLI on the router, and then retry this task, starting with Step 2.
Step 6	**boot flash** **Example:** `ServicesEngine boot-loader> boot flash`	Loads the NAM helper image. • This command is entered in the boot loader CLI, which is separate from the NAM CLI and Cisco IOS CLI.
Step 7	When prompted to select from the helper menu, enter **6**. **Example:** `Selection [12345678rh]: 6`	Selects the menu option to reset the root password to the default value of "root".

	Command or Action	Purpose
Step 8	When prompted to select from the helper menu, enter **r**. **Example:** `Selection [12345678rh]:r`	Selects the menu option to exit the helper and reset the NAM.

Step 9	**`y`**
	Example:
	`About to exit and reset Services Engine.`
	`Are you sure? [y/N] y`
		Confirms that you want to exit the helper and reset the NAM.
		• This time, ignore the prompt to enter ***.

Step 10	Hold **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.
	Example:
	`login: <suspend keystroke>`
	`Router#`
		Suspends and closes the Telnet session.

Step 11	**`disconnect`**
	Example:
	`Router# disconnect`
		Disconnects a line.

Step 12	Press **Enter**.
	Example:
	`Closing connection to 10.20.30.40 [confirm]`
	`<Enter>`
		Confirms that you want to disconnect the line.

Example

This section provides the following example:

- Resetting the NAM Root Password to the Default Value: Example, page 606

Resetting the NAM Root Password to the Default Value: Example

```
Router# service-module analysis-module 1/0 reload
Do you want to proceed with reload?[confirm] y
Trying to reload Service Module Analysis-Module1/0.

Router# service-module analysis-module 1/0 session
Trying 172.20.104.87, 2033 ... Open
.
<debug output omitted>
.
Booting from flash..., please wait.

[BOOT-ASM]
7

Please enter '***' to change boot configuration: ***

 ServicesEngine Bootloader Version :1.0.6aN
ServicesEngine boot-loader> boot flash
.
<debug output omitted>
.
==============================================================================
Cisco Systems, Inc.
Services engine helper utility for NM-NAM
Version 1.1(1) [200311111641]

-----
Main menu
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Download bootloader and write to flash
4 - Download helper and write to flash
5 - Display software versions
6 - Reset application image CLI passwords to default
7 - Change file transfer method (currently ftp/http)
8 - Show upgrade log
9 - Send Ping
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine

Selection [123456789rh]: 6
Restored default CLI passwords of application image.
==============================================================================
Cisco Systems, Inc.
Services engine helper utility for NM-NAM
Version 1.1(1) [200311111641]

-----
Main menu
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Download bootloader and write to flash
4 - Download helper and write to flash
5 - Display software versions
6 - Reset application image CLI passwords to default
7 - Change file transfer method (currently ftp/http)
8 - Show upgrade log
9 - Send Ping
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine

Selection [123456789rh]: r
About to exit and reset Services Engine.
Are you sure? [y/N] y
INITSending all processes the TERM signal...
Sending all processes the KILL signal...
Unmounting file systems:
Please stand by while rebooting the system...
Restarting system.
.
<debug output omitted>
.
Cisco Network Analysis Module (NM-NAM)

nam1.cisco.com login: <suspend keystroke>
Router#
Router# disconnect
Closing connection to 10.1.1.1 [confirm] <Enter>
Deleting login session
```

Troubleshooting Tips

If you have trouble opening a NAM console session from the router, make sure that the NAM console line is clear by entering the **service-module analysis-module** *slot*/**0 session clear** command in privileged EXEC mode.

What to Do Next

Verify that the default root password of "root" is accepted by performing Step 1 through Step 5 in the "Opening and Closing a NAM Console Session from the Router" section on page 588.

To change the NAM root password, see the "Changing the NAM Root Password" section on page 602.

Opening and Closing a Telnet or SSH Session to the NAM

This section describes how to open and close a Telnet or SSH session to the NAM. This task is not commonly performed, because you would typically use the NAM Traffic Analyzer (web GUI) to monitor and maintain the NAM. If, however, you cannot access the NAM Traffic Analyzer, then you might want to use Telnet or SSH to troubleshoot from the NAM CLI.

If your NM-NAM is not properly configured for Telnet or SSH access (see the following Prerequisites section), then you can open a Telnet session to the router in which the NM-NAM is installed, and then open a NAM console session from the router. See the "Opening and Closing a NAM Console Session from the Router" section on page 588.

Prerequisites

- Configure the NAM system IP address. Optionally, set the NAM system hostname. See the "Configuring the NM-NAM" section on page 591.
- Verify NAM network connectivity by performing one of the following ping tests:
  - From a host beyond the gateway, ping the NAM system IP address.
  - From the NAM CLI, ping the NAM system default gateway.

Telnet Prerequisites

- Enter the **exsession on** NAM CLI command. See Step 5 of the "Configuring the NM-NAM" section on page 591.

SSH Prerequisites

- Install the NAM software K9 crypto patch, which you can download from Cisco.com.
- Enter the **exsession on ssh** NAM CLI command. See Step 5 of the "Configuring the NM-NAM" section on page 591.

SUMMARY STEPS

1. **telnet** {*ip-address* | *hostname*}
   or
   ssh {*ip-address* | *hostname*}
2. At the login prompt, enter **root**.
3. At the password prompt, enter your password.
   or
   If you have not changed the password from the factory-set default, enter **root** as the root password.
4. Perform the tasks that you need to perform in the NAM CLI. When you want to end the Telnet or SSH session to the NAM and return to the Cisco IOS CLI, complete Step 5 and Step 6.
5. **exit**
6. **logout**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`telnet`** `{`*`ip-address`*` | `*`hostname`*`}`
	or
	`ssh` `{`*`ip-address`*` | `*`hostname`*`}`
	Example:
	`Router# telnet 10.20.30.40`
	Example:
	`Router# ssh 10.20.30.40`
		Logs in to a host that supports Telnet.
		or
		Starts an encrypted session with a remote networking device.
		• Use the NAM system IP address or NAM system hostname.

Step 2	At the login prompt, enter **root**. **Example:** `login: root`	Accesses the root (read/write) level of NAM.
Step 3	At the password prompt, enter your password. or If you have not changed the password from the factory-set default, enter **root** as the root password. **Example:** `Password: root`	—
Step 4	Perform the tasks that you need to perform in the NAM CLI. When you want to end the Telnet or SSH session to the NAM and return to the Cisco IOS CLI, complete Step 5 and Step 6.	For help using NAM CLI commands, see the "NAM CLI Context-Sensitive Help" section on page 582.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`root@localhost(sub-custom-filter-capture)# exit`
	`root@localhost#`
		Leaves a subcommand mode.
		• Return to command mode.

Step 6	**logout**
	Example:
	`root@localhost# logout`
	`Connection closed by foreign host.`
		Logs out of the NAM system.

Examples

This section provides the following examples:

- Opening and Closing a Telnet Session to the NAM Using the NAM System IP Address: Example, page 610
- Opening and Closing an SSH Session to the NAM Using the NAM System Hostname: Example, page 610

Opening and Closing a Telnet Session to the NAM Using the NAM System IP Address: Example

```
Router> telnet 172.20.105.215
Trying 172.20.105.215 ... Open

Cisco Network Analysis Module (NM-NAM)

login: root
Password: <password>
Terminal type: vt100

Cisco Network Analysis Module (NM-NAM) Console, 3.2
Copyright (c) 1999-2003 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@nam.cisco.com#
root@nam.cisco.com# logout

[Connection to 172.20.105.215 closed by foreign host]
Router>
```

Opening and Closing an SSH Session to the NAM Using the NAM System Hostname: Example

```
host [/home/user] ssh -l root nmnam2
root@nmnam2's password: <password>
Terminal type: vt100

Cisco Network Analysis Module (NM-NAM) Console, 3.2
Copyright (c) 1999-2003 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@nmnam2.cisco.com#
root@nmnam2.cisco.com# logout

Connection to nmnam2 closed.
host [/home/user]
```

Upgrading the NAM Software

This section describes how to upgrade the NAM software. This task is performed from the NAM CLI.

NAM Software Images

The NM-NAM contains three NAM software images:

- NAM application image on the hard drive—Source of the NAM Traffic Analyzer and NAM CLI
- Helper image in flash memory—Used to recover or upgrade NAM software images
- Bootloader image in flash memory—Used to specify whether to boot the NAM application image or the helper image

Types of NAM Software Upgrades

NAM software upgrades are available in two forms:

- Patches—Incremental updates to software releases that are installed with the **patch** NAM CLI command. Patches are available only for the NAM application image.
- Images—Full image releases that are installed from the helper image. Full image upgrades are typically used to update the NAM application image, but if necessary and recommended by technical support, you can also use the helper image to upgrade the bootloader image or helper image.

Prerequisites

- Download the NAM software image from Cisco.com, and copy the image to an FTP server.
- Before performing this task, access the NAM console by completing Step 1 through Step 5 in the "Opening and Closing a NAM Console Session from the Router" section on page 588.

Perform one of the following tasks in this section, depending on whether you are adding a patch to your NAM application or are performing a full software image upgrade:

- Upgrading the NAM Software—Patch, page 611
- Upgrading the NAM Software—Full Image, page 612

Upgrading the NAM Software—Patch

Perform this task to add a patch to your NAM application image. This task is performed from the NAM CLI.

SUMMARY STEPS

1. **patch** *ftp://user:passwd@host/full-path/filename*
   or
   patch *ftp://user@host/full-path/filename*
2. **show patches**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**patch** *ftp://user:password@host/full-path/filename*
	or
	patch *ftp://user@host/full-path/filename*
	Example:
	`root@nam1.cisco.com# patch ftp://person:mypwd@examplehost/dir/subdir/nam-app.3-2.cryptoK9.patch.1-0.bin`
	Example:
	`root@nam1.cisco.com# patch ftp://person@examplehost/dir/subdir/nam-app.3-2.cryptoK9.patch.1-0.bin`
	`Proceeding with installation. Please do not interrupt.`
	`If installation is interrupted, please try again.`
	`Downloading nam-app.3-2.cryptoK9.patch.1-0.bin. Please wait...`
	`Password for person@examplehost: <mypwd>`
		Downloads and installs a software patch.
		• Use the first option, which includes the password, if the FTP server does not allow anonymous users.
		• If you use the second option, enter your password when prompted.
		• Remember to perform this task in the NAM CLI.

Step 2	**show patches** **Example:** `root@nam1.cisco.com# show patches`	Displays all installed patches. • Verify that your patch was successfully installed.

Upgrading the NAM Software—Full Image

Perform this task to upgrade one of your NAM software images to a new release. This task is performed from the NAM CLI.

SUMMARY STEPS

1. **reboot**
2. **y**
3. When prompted, enter *** to change the boot configuration.
4. **boot flash**
5. When prompted to select from the helper menu, enter **1**.
6. **ftp://***ip-address***/***path***/***nam-image-file*
7. **y**
8. **r**
9. **y**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`reboot`**
	Example:
	`root@nam1.cisco.com# reboot`
		Shuts down and restarts the NAM.
		• Remember to perform this task in the NAM CLI.

Step 2	**`y`**
	Example:
	`Reboot the NAM? (Y/N) [N]: y`
		Confirms that you want to reboot the NAM.
		• After you confirm the reboot, the NAM displays a series of messages as it stops processes, shuts down, and then restarts.

Step 3	When prompted, enter *** to change the boot configuration. **Example:** `Please enter '***' to change boot configuration: ***`	Interrupts the boot loader. • Enter *** immediately after the prompt appears. • If you do not enter the *** in time to interrupt the boot loader, then return to Step 1 and try again.

Step 4	**`boot flash`**
	Example:
	`ServicesEngine boot-loader> boot flash`
		Loads the NAM helper image.
		• This command is entered in the boot loader CLI, which is separate from the NAM CLI and Cisco IOS CLI.

Step 5	When prompted to select from the helper menu, enter **1** or **2**.
	Example:
	`Selection [12345678rh]: 1`
	Example:
	`Selection [12345678rh]: 2`
		Selects the menu option to download the NAM software image onto the NM-NAM internal memory.
		• Option 1 preserves all configuration and report data while installing the NAM software image.
		• Option 2 reformats the NM-NAM hard drive, deleting all report data and NAM software configurations, except the basic IP configuration. Although useful for recovering a corrupted hard drive, Option 2 should be used with caution or when recommended by technical support.
		• The helper menu also has an option (7) to change the file transfer method from the default FTP method. Before performing Step 5, you may enter 7 to select the TFTP transfer method. Because many TFTP servers have problems transferring files as large as the NAM application image, we recommend that you use the default FTP method.

Step 6	**`ftp://`***`ip-address`***`/`***`path`***`/`***`nam-image-file`*
	Example:
	`Download NAM application image via ftp and write to HDD`
	`URL of application image []:`
	`ftp://172.20.98.136/dir1/dir2/nam-image.bin.gz`
		Specifies the FTP location and filename of the NAM software image.

	Command or Action	Purpose
Step 7	**y** **Example:** `Do you want to proceed installing it? [y/N] y`	Confirms that you want to install the specified NAM software image.
Step 8	**r** **Example:** `Selection [12345678rh]:r`	Selects the menu option to exit the helper and reset the NAM.

Step 9	**y**
	Example:
	`About to exit and reset Services Engine.`
	`Are you sure? [y/N] y`
		Confirms that you want to exit the helper and reset the NAM.
		• This time, ignore the prompt to enter ***.

Examples

This section provides the following examples:

- Upgrading the NAM Software—Patch: Example, page 614
- Upgrading the NAM Software—Full Image: Example, page 615

Upgrading the NAM Software—Patch: Example

```
Router> enable
Password: <password>
Router#
Router# service-module analysis-Module 1/0 session
Trying 172.20.104.86, 2033 ... Open

Cisco Network Analysis Module (NM-NAM)

nam1.cisco.com login: root
Password: <password>
Terminal type:vt100

Cisco Network Analysis Module (NM-NAM) Console, 3.2(0.10)
Copyright (c) 1999-2003 by cisco Systems, Inc.

WARNING! Default password has not been changed!

root@nam1.cisco.com# patch
ftp://person@examplehost/dir/subdir/nam-app.3-2.cryptoK9.patch.1-0.bin

Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading nam-app.3-2.cryptoK9.patch.1-0.bin. Please wait...
Password for person@examplehost: <mypwd>
ftp://person@examplehost/dir/subdir/nam-app.3-2.cryptoK9.patch.1-0.bin
(1K)
/usr/local/nam/patch/wor  [########################]       1K |  104.43K/s
1894 bytes transferred in 0.02 sec (102.35k/sec)

Verifying nam-app.3-2.cryptoK9.patch.1-0.bin. Please wait...
Patch nam-app.3-2.cryptoK9.patch.1-0.bin verified.
```

```
Applying /usr/local/nam/patch/workdir/nam-app.3-2.cryptoK9.patch.1-0.bin.
Please wait...
########################################### [100%]
########################################### [100%]

Patch applied successfully.
root@nam1.cisco.com# show patches

Tue Aug 31 21:04:28 2004 Patch:nam-app.3-2.strong-crypto-patchK9-1-0
Description:Strong Crypto Patch for NAM.

root@nam1.cisco.com#
```

Upgrading the NAM Software—Full Image: Example

```
Router> enable
Password: <password>
Router#
Router# service-module analysis-Module 1/0 session
Trying 172.20.104.86, 2033 ... Open

Cisco Network Analysis Module (NM-NAM)

nam1.cisco.com login: root
Password: <password>
Terminal type:vt100

Cisco Network Analysis Module (NM-NAM) Console, 3.2(0.10)
Copyright (c) 1999-2003 by cisco Systems, Inc.

WARNING! Default password has not been changed!

root@nam1.cisco.com#
root@nam1.cisco.com# reboot
Reboot the NAM? (Y/N) [N]: y

System reboot in process...
.
<debug output omitted>
.
Booting from flash..., please wait.

[BOOT-ASM]
7

Please enter '***' to change boot configuration: ***

 ServicesEngine Bootloader Version :1.0.6-NAM

ServicesEngine boot-loader>
ServicesEngine boot-loader> boot flash
.
<debug output omitted>
.
==============================================================================
Cisco Systems, Inc.
Services engine helper utility for NM-NAM
Version 1.1(1) [200311111641]

-----
```

```
Main menu
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Download bootloader and write to flash
4 - Download helper and write to flash
5 - Display software versions
6 - Reset application image CLI passwords to default
7 - Change file transfer method (currently ftp/http)
8 - Show upgrade log
9 - Send Ping
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine

Selection [123456789rh]: 1


-----
Download NAM application image via ftp and write to HDD
URL of application image []: ftp://172.20.98.136/dir1/dir2/nam-image.bin.gz
Getting c6svc-nam.mainline-DAILY_20030825.bin.gz from 171.69.17.19 via ftp.
ftp://172.20.98.136/dir1/dir2/nam-image.bin.gz
(46389K)
-                          [########################]   46389K | 7421.38K/s
47502347 bytes transferred in 6.25 sec (7421.14k/sec)
upgrade.bin size:48241545
File transfer successful.
Checking upgrade.bin
Do you want to proceed installing it? [y/N] y
.
<debug output omitted>
.
Application image upgrade complete. You can boot the image now.
==============================================================================
Cisco Systems, Inc.
Services engine helper utility for NM-NAM
Version 1.1(1) [200311111641]

-----
Main menu
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Download bootloader and write to flash
4 - Download helper and write to flash
5 - Display software versions
6 - Reset application image CLI passwords to default
7 - Change file transfer method (currently ftp/http)
8 - Show upgrade log
9 - Send Ping
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine

Selection [123456789rh]: r
About to exit and reset Services Engine.
Are you sure? [y/N] y
```

Troubleshooting Tips

If you have trouble opening a NAM console session from the router, make sure that the NAM console line is clear by entering the **service-module analysis-module** *slot*/**0 session clear** command in privileged EXEC mode.

Configuration Examples for the Network Analysis Module (NM-NAM)

This section provides the following configuration examples:

- NAM Management Interface Is Internal and Analysis-Module Interface Is Assigned an IP Address: Example, page 617
- NAM Management Interface Is Internal and Analysis-Module Interface Is IP Unnumbered: Example, page 619
- NAM Management Interface Is External and Analysis-Module Interface Is IP Unnumbered: Example, page 621

NAM Management Interface Is Internal and Analysis-Module Interface Is Assigned an IP Address: Example

In this configuration example:

- The internal NAM interface is used for management traffic.
- IP addresses from the same routable subnet are assigned to the Analysis-Module interface and the NAM system.
- A static route to the NAM through the Analysis-Module interface is configured.
- The internal NAM interface is used to monitor WAN traffic on interface Serial 0/0, and the external NAM interface is used to monitor LAN traffic on interface Fast Ethernet 0/0.
- The NM-NAM is installed in router slot 2.

Figure 60 shows the topology used in the example, and the following sections show the router and NAM configurations:

- Router Configuration (Cisco IOS Software), page 618
- NAM Configuration (NAM Software), page 619

Figure 60 ***NAM Management Interface Is Internal and Analysis-Module Interface Is Assigned an IP Address***

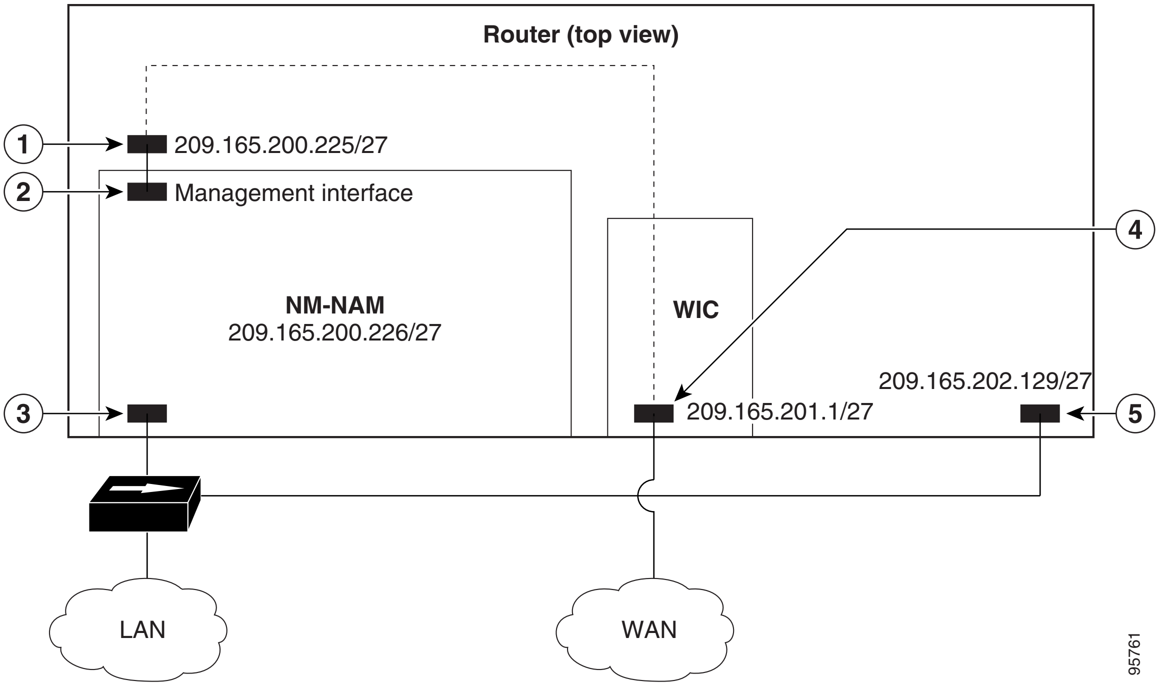


Figure 60 Callout	Interface	Location
1	Analysis-Module interface	Router internal
2	Internal NAM interface (**management**)	NM-NAM internal
3	External NAM interface	NM-NAM faceplate
4	Serial interface	WAN interface card (WIC)
5	Fast Ethernet interface	Router rear panel

Router Configuration (Cisco IOS Software)

```
!
ip cef
!
ip route 209.165.200.226 255.255.255.224 analysis-module 2/0
!
interface FastEthernet0/0
 ip address 209.165.202.129 255.255.255.224
 ip route-cache flow
 speed auto
 full-duplex
 no mop enabled
 no shutdown
!
interface Serial 0/0
 encapsulation ppp
 ip address 209.165.201.1 255.255.255.224
 analysis-module monitoring
 no shutdown
```

```
!
interface analysis-module 2/0
 ip address 209.165.200.225 255.255.255.224
 hold-queue 60 out
 no shutdown
!
```

NAM Configuration (NAM Software)

```
!
ip address 209.165.200.226 255.255.255.224
!
ip host "nam1"
!
ip domain "cisco.com"
!
ip gateway 209.165.200.225
!
ip broadcast 10.255.255.255
!
ip nameserver 172.16.201.29
!
ip interface internal
!
ip http server enable
!
exsession on
!
```

NAM Management Interface Is Internal and Analysis-Module Interface Is IP Unnumbered: Example

In this configuration example:

- The internal NAM interface is used for management traffic.
- IP addresses from the same routable subnet are assigned to the Analysis-Module interface and the NAM system.
- To conserve IP address space, the Analysis-Module interface is configured as IP unnumbered to borrow the IP address of the Fast Ethernet interface.
- A static route to the NAM through the Analysis-Module interface is configured.
- The internal NAM interface is used to monitor WAN traffic on interface Serial 0/0, and the external NAM interface is used to monitor LAN traffic on interface Fast Ethernet 0/0.
- The NM-NAM is installed in router slot 2.

Figure 61 shows the topology used in the example, and the following sections show the router and NAM configurations:

- Router Configuration (Cisco IOS Software), page 620
- NAM Configuration (NAM Software), page 621

Figure 61 Sample Topology: NAM Management Interface Is Internal and Analysis-Module Interface Is IP Unnumbered

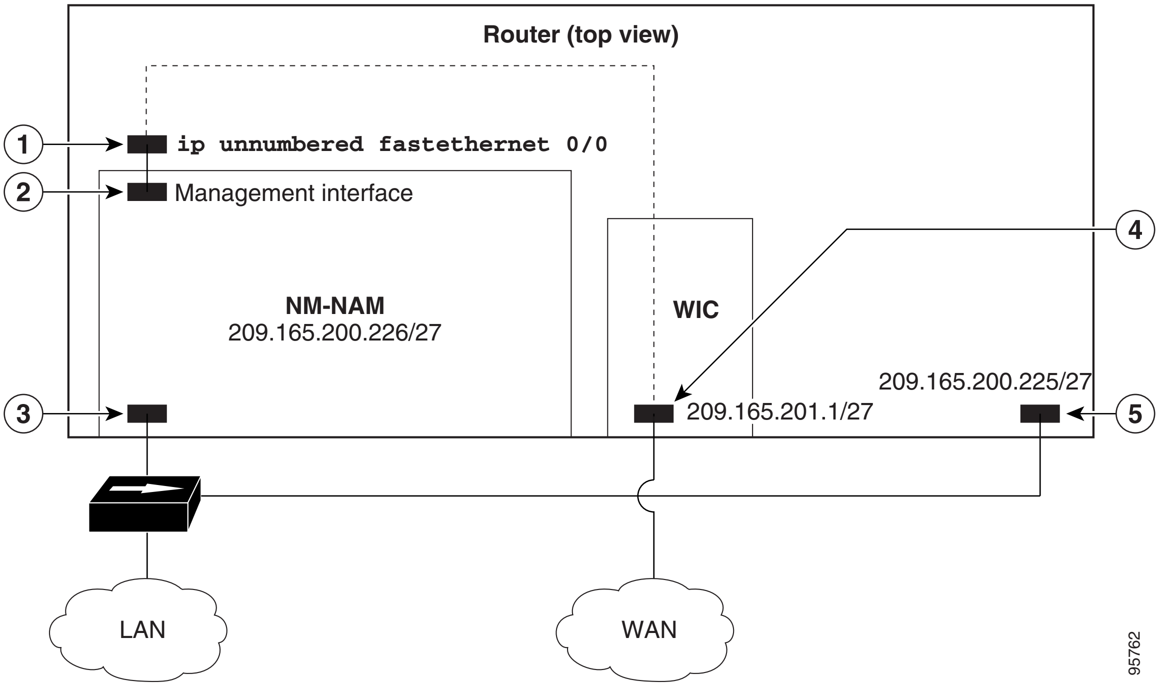


Figure 61 Callout	Interface	Location
1	Analysis-Module interface	Router internal
2	Internal NAM interface (**management**)	NM-NAM internal
3	External NAM interface	NM-NAM faceplate
4	Serial interface	WAN interface card (WIC)
5	Fast Ethernet interface	Router rear panel

Router Configuration (Cisco IOS Software)

```
!
ip cef
!
ip route 209.165.200.226 255.255.255.224 analysis-module 2/0
!
interface FastEthernet0/0
 ip address 209.165.200.225 255.255.255.224
 ip route-cache flow
 speed auto
 full-duplex
 no mop enabled
 no shutdown
!
interface Serial 0/0
 encapsulation ppp
 ip address 209.165.201.1 255.255.255.224
 analysis-module monitoring
 no shutdown
```

```
!
interface analysis-module 2/0
 ip unnumbered FastEthernet0/0
 no shutdown
 hold-queue 60 out
!
```

NAM Configuration (NAM Software)

```
!
ip address 209.165.200.226 255.255.255.224
!
ip host "nam1"
!
ip domain "cisco.com"
!
ip gateway 209.165.200.225
!
ip broadcast 10.255.255.255
!
ip nameserver 172.16.201.29
!
ip interface internal
!
ip http server enable
!
exsession on
!
```

NAM Management Interface Is External and Analysis-Module Interface Is IP Unnumbered: Example

In this configuration example:

- The external NAM interface is used for management traffic.
- The Analysis-Module interface is configured as IP unnumbered to borrow the IP address of the loopback interface.
- The borrowed loopback interface IP address is not routable.
- The NAM system is configured with an IP address from the LAN subnet that is connected to the external NAM interface.
- The internal NAM interface is used to monitor WAN traffic on interface Serial 0/0, and the external NAM interface is used to monitor LAN traffic on interface Fast Ethernet 0/0.
- The NM-NAM is installed in router slot 3.

Figure 62 shows the topology used in the example, and the following sections show the router and NAM configurations:

- Router Configuration (Cisco IOS Software), page 622
- NAM Configuration (NAM software), page 623

Figure 62 Sample Topology: NAM Management Interface Is External and Analysis-Module Interface Is IP Unnumbered

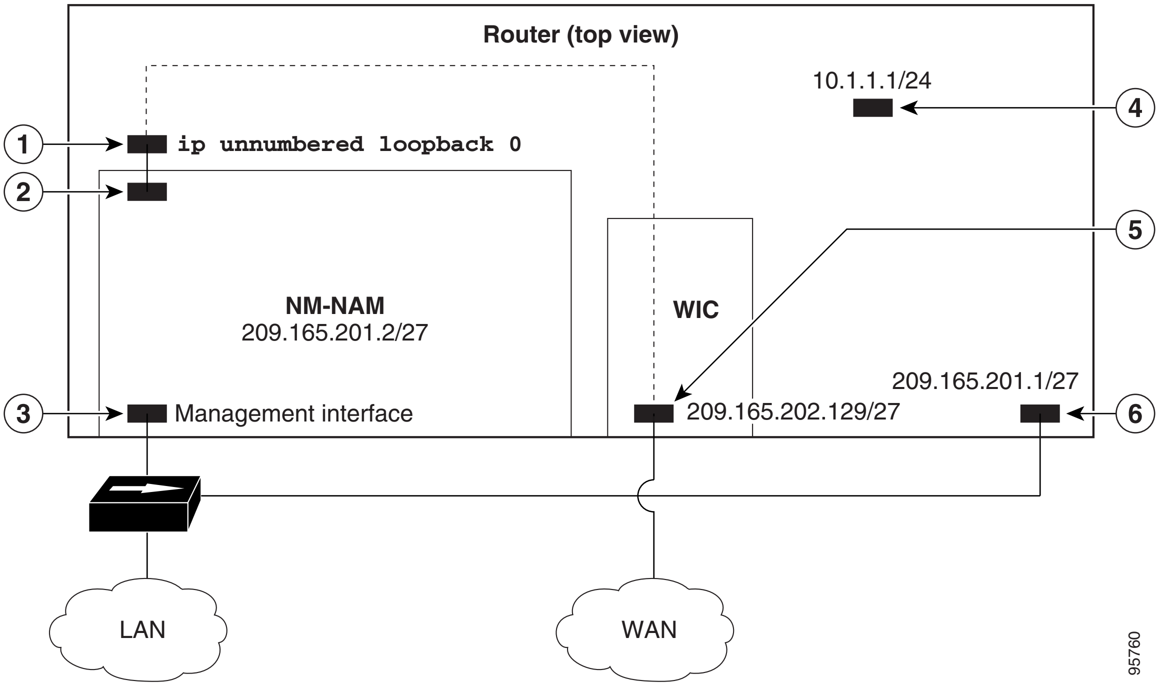


Figure 62 Callout	Interface	Location
1	Analysis-Module interface	Router internal
2	Internal NAM interface	NM-NAM internal
3	External NAM interface (**management**)	NM-NAM faceplate
4	Loopback interface	Router internal
5	Serial interface	WAN interface card (WIC)
6	Fast Ethernet interface	Router rear panel

Router Configuration (Cisco IOS Software)

```
!
ip cef
!
interface loopback 0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 209.165.201.1 255.255.255.224
 ip route-cache flow
 speed auto
 full-duplex
 no mop enabled
 no shutdown
```

```
!
interface Serial 0/0
 encapsulation ppp
 ip address 209.165.202.129 255.255.255.224
 analysis-module monitoring
 no shutdown
!
interface analysis-module 3/0
 ip unnumbered loopback 0
 hold-queue 60 out
 no shutdown
!
```

NAM Configuration (NAM software)

```
!
ip address 209.165.201.2 255.255.255.224
!
ip host "nam1"
!
ip domain "cisco.com"
!
ip gateway 209.165.201.1
!
ip broadcast 10.255.255.255
!
ip nameserver 209.165.201.29
!
ip interface external
!
ip http server enable
!
exsession on
!
```

Additional References

The following sections provide references related to the Network Analysis Module (NM-NAM) feature.

Related Documents

Related Topic	Document Title
Compatibility matrixes for NAM software releases, Cisco IOS releases, and platforms Links to software downloads, product documentation, and technical documentation, including NAM software release notes, user guide, and command reference	Cisco Network Analysis Module (NAM)
Installing and cabling network modules	*Cisco Network Modules Hardware Installation Guide*
Safety and compliance	*Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*
Cisco IOS interface commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Interface and Hardware Component Command Reference*

Related Topic	Document Title
Router documentation	Modular Access Routers
IP unnumbered interfaces	*Understanding and Configuring the ip unnumbered Command*
Authentication, authorization, and accounting (AAA)	*Cisco IOS Security Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
Router MIBs: • CISCO-ENTITY-VENDORTYPE-OID-MIB Network Analysis Module (NAM) MIBs: • ART-MIB • DSMON-MIB • HC-RMON-MIB • MIB-II • RMON-MIB • RMON2-MIB • SMON-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2021	*Remote Network Monitoring Management Information Base Version 2 using SMIv2*
RFC 2074	*Remote Network Monitoring MIB Protocol Identifiers*
RFC 2613	*Remote Network Monitoring MIB Extensions for Switch Networks Version 1.0*
RFC 2819	*Remote Network Monitoring Management Information Base*
RFC 3273	*Remote Network Monitoring Management Information Base for High Capacity Networks*
RFC 3287	*Remote Monitoring MIB Extensions for Differentiated Services*

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 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.

- **analysis-module monitoring**
- **interface analysis-module**
- **service-module analysis-module reload**
- **service-module analysis-module reset**
- **service-module analysis-module session**
- **service-module analysis-module shutdown**
- **service-module analysis-module status**
- **show controllers analysis-module**
- **show interfaces analysis-module**

Glossary

AAA—authentication, authorization, and accounting. Pronounced “triple a.”

access list—A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

CEF—Cisco Express Forwarding.

DSMON—Differentiated Services Monitoring.

flooding—Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.

GRE—generic routing encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

GUI—graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.

IP multicast—Routing technique that allows IP traffic to be propagated from one source to a number of destinations or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to a multicast group identified by a single IP destination group address.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

NAT—Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as *Network Address Translator.*

NetFlow—A feature of some routers that allows them to categorize incoming packets into flows. Because packets in a flow often can be treated in the same way, this classification can be used to bypass some of the work of the router and accelerate its switching operation.

PCI—Peripheral Component Interconnect. An industry local bus standard.

QoS—quality of service. Cisco IOS QoS technology lets complex networks control and predictably service a variety of networked applications and traffic types.

RMON—remote monitoring. MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.

SNMP—Simple Network Management Protocol. Network 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. SNMPv2c supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

SSH—Secure Shell Protocol. A protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

VoIP—Voice over IP. The capability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the digital signal processor (DSP) segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

Note Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

Minimal Disruptive Restart of VIP Cards

The Minimal Disruptive Restart (MDR) of VIP Cards feature optimizes the reload time of a VIP card on a Cisco 7500 series router after a software failure has occurred. The amount of time for a VIP card to reload with the MDR functionality varies depending on the port adapter in the VIP card. With this software enhancement, the reload time of a VIP card with the Single Line Card Reload (SLCR) technology is decreased from approximately 30 seconds to approximately 5 seconds. This improvement provides high availability and minimizes equipment downtime. As an additional part of this feature, users can initiate a VIP card reload with the MDR functionality on a single slot using the **microcode reload** command.

The MDR functionality has the following limitations:

- If a VIP card software failure occurs within 5 minutes of up time, the VIP card is not reloaded with the MDR functionality. Instead, a standard reset and microcode reload is performed. If a software failure occurs after 5 minutes of up time, the VIP card is reloaded with the MDR functionality.
- A VIP card can be reloaded with the MDR functionality five consecutive times. If a VIP card must be reloaded for a sixth consecutive time, it is not reloaded with the MDR functionality. Instead, a standard reset and microcode reload is performed.

These limitations are not applicable when performing a VIP card reload using the **microcode reload** command. There is no limit to the number of times a VIP card can be reloaded with this command.

Feature History for the Minimal Disruptive Reload of VIP Cards Feature

Release	Modification
12.3(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.

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.

- **microcode reload (7500)**

ATM Mode for Two-Wire or Four-Wire SHDSL

This document describes the ATM Mode for Two-Wire or Four-Wire SHDSL feature on the Cisco 1700 series, Cisco 1800 series, Cisco 2600 series, Cisco 2800, Cisco 3631, Cisco 3700, and Cisco 3800 series routers.

The ATM Mode for Two-Wire or Four-Wire SHDSL feature adds four-wire support in fixed line-rate mode only on a WIC-1SHDSL-V2. Two-wire mode supports two-wire line-rate and auto line-rate. This feature builds on the existing features of the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WAN interface card (WIC-1SHDSL). The four-wire feature of G.991.2 doubles the bandwidth in ATM mode and increases usable distance over two pairs of wires.

The WIC-1SHDSL-V2 supports ATM on two-wire and four-wire line mode. Embedded Operation Channel (EOC) messages support for customer premise equipment (CPE) is provided for two-wire and four-wire modes.

Feature Specifications for the ATM Mode for SHDSL

Feature History	
Release	**Modification**
12.3(4)XD	This feature (WIC-1SHDSL-V2) was introduced on the Cisco 2600 series and Cisco 3700 series routers to add four-wire support. Two-wire support was previously available in *1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers*, Release 12.2(8)T.
12.3(4)XG	This feature (WIC-1SHDSL-V2) was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This feature (WIC-1SHDSL-V2) was integrated into the Cisco IOS Release 12.3(7)T on the Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers. Cisco 1700 series routers do not support the WIC-1SHDSL-V2 in this release.
12.3(4)XG1	Support for the auto line-mode feature was added.
12.3(11)T	Support for the following was added: additional annex parameters for Cisco 1700, Cisco 2600, Cisco 2800, Cisco 3631, Cisco 3700, and Cisco 3800 series routers; the HDSL2-SHDSL-LINE-MIB (RFC3276); and support for the ATM Mode for SHDSL feature was added for Cisco 2800 series, and Cisco 3800 series routers.
12.3(14)T	Support was added for Cisco 1800 series routers and the Cisco 2801 Integrated Services router.

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 Mode for Two-Wire or Four-Wire SHDSL

- A G.SHDSL WIC must be installed in the router to match the DSL service to be configured.
- Minimum memory recommendations are shown in Table 35.

Table 35 Minimum Memory Recommendations for ATM Mode for Two-Wire or Four-Wire SHDSL

Platform Name	Image Name	Flash Memory Recommended	DRAM Memory Recommended
Cisco 1700 Series	IOS IP BASE	16 MB	64 MB
Cisco 1800 Series	IOS IP BASE	16 MB	64 MB
Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM	IOS IP BASE	16 MB	64 MB
Cisco 2691	IOS IP BASE	32 MB	128 MB
Cisco 2800 Series	IOS IP BASE	32 MB	128 MB
Cisco 3631	IOS IP BASE	32 MB	128 MB
Cisco 3725	IOS IP BASE	32 MB	128 MB
Cisco 3745	IOS IP BASE	32 MB	128 MB
Cisco 3800 Series	IOS IP BASE	32 MB	128 MB

Restrictions for ATM Mode for Two-Wire or Four-Wire SHDSL

- The *auto* parameter of the **line-mode** command on the WIC-1SHDSL-V2 is supported only in Cisco IOS Release 12.3(4)XG1 and later releases.
- The WIC-1SHDSL-V2 ATM Mode for SHDSL does not support ATM adaption layer 1 (AAL1) and/or circuit emulation service.
- ATM adaption layer 2 (AAL2) is not supported on Cisco 1700 series, and Cisco 2801 routers.
- The ATM Mode for SHDSL does not interface with AIM-ATM.
- The ATM Mode for SHDSL does not support available bit rate (ABR) class of service (CoS).
- The ATM Mode for SHDSL does not support unspecified bit rate plus (UBR+).
- The ATM Mode for SHDSL only support 23 private virtual circuits (PVC) per WIC.
- The WIC-1SHDSL-V2 should be inserted only into onboard WIC slots or NM-2W, NM-1FE2W, NM-1FE1R2W, NM-2FE2W, NM-1FE2W-V2, or NM-2FE2W-V2 network modules. This WIC is not supported in NM-1E2W, NM-1E1R-2W, or NM-2E2W combination network modules.
- The WIC-1SHDSL-V2 does not support T1/E1 mode in four-wire mode.
- The WIC-1SHDSL does not support T1/E1 mode.

Information About ATM Mode for Two-Wire or Four-Wire SHDSL

This section provides information about the ATM Mode for SHDSL feature.

- SHDSL Features, page 633
- ATM Features, page 634
- Interface and Controller Numbering on the Cisco 1721 Router, page 634
- Interface Numbering on Cisco 2800 and Cisco 3800 Series Routers, page 635

SHDSL Features

Supported SHDSL features are listed as follows:

- ITU G.991.2 support (full support for Annex A & B)
  - Dying Gasp (ITU G.991.2) is supported.
  - Terminating wetting current is supported.
  - Two-wire mode supports speeds from 192 kbps to 2.304 Mbps in increments of 64 kbps in both fixed and auto line rate.
  - Four-wire mode supports speeds from 384 kbps to 4.608 Mbps in increments of 128 kbps in fixed line rate only and provides increased rate capability and greater reach.

ATM Features

The supported ATM features in this release:

- Provide ATM traffic management to enable service providers to manage their core ATM network infrastructures.
- Support ATM class of service features constant bit rate (CBR), variable bit rate-nonreal time (VBR-nrt), variable bit rate-real time (VBR-rt), and unspecified bit rate (UBR).
- Operate back-to-back or through a digital subscriber line access multiplexer (DSLAM).
- Provide toll-quality Voice over IP delivery over AAL5.
- Support VoATM over AAL2, but AAL2 is not supported on the Cisco 1700 series routers.
- Support VoATM over AAL5.

Interface and Controller Numbering on the Cisco 1721 Router

If a WIC-1SHDSL-V2 is installed in a Cisco 1721 router, the interfaces and controllers are assigned numbers based on a numbering scheme that is different from the slot numbering scheme on other Cisco routers. This is because the Cisco 1721 router assigns only a slot number without also assigning a port number. Other Cisco routers typically use a slot and port number combination.

If the WIC-1SHDSL-V2 (the DSL controller) is installed in slot 0, the T1/E1 controllers and the ATM interfaces (ADSL/SHDSL) will be numbered relative to the DSL controller in slot 0. See Table 36 for examples of the slot numbering scheme on the Cisco 1721 router.

With an ATM or MFT T1/E1 card in slot 0, the WIC-1SHDSL-V2 in slot 1 will be numbered relative to the number of ports in slot 0.

If both slots are occupied by DSL controllers, the logical interfaces configured on each controller will have the same number as the slot occupied by the DSL controller. All logical interfaces on the WIC-1SHDSL-V2, such as serial interfaces created during the configuration of channel groups in T1/E1 mode, will have the same number as the DSL controller.

Table 36 Examples of Slot Numbering on the Cisco 1721 Router

Interface Cards and Controllers Installed	Slot Numbering Assignment

A WIC-1SHDSL-V2 is in slot 0, and an MFT-T1/E1 is installed in the other slot, which will be numbered as slot 1.	For WIC-1SHDSL-V2:
	`controller dsl 0`
	`interface atm0 (or controller t1 0)`
	For MFT-T1:
	`controller t1 1`

A WIC-1SHDSL-V2 is in slot 0, and an ADSL/SHDSL WIC is in slot 1.	For WIC-1SHDSL-V2:
	`controller dsl 0, interface atm0 (or controller t1 0)`
	For ADSL/SHDSL WIC:
	`interface atm 1`

Table 36 Examples of Slot Numbering on the Cisco 1721 Router (continued)

Interface Cards and Controllers Installed	Slot Numbering Assignment

An ATM or MFT T1/E1 card is in slot 0, and a WIC-1SHDSL-V2 is in slot 1. The WIC-1SHDSL-V2 will be numbered relative to the ports in slot 0.	For ADSL/SHDSL:
	`interface atm 0`
	For WIC-1SHDSL-V2:
	`controller dsl 1, interface atm 1 (or controller t1 1)`

A 1MFT-T1/E1 is in slot 0, and a WIC-1SHDSL-V2 is in slot 1.	For 1MFT-T1/E1:
	`controller t1 0`
	For WIC-1SHDSL-V2:
	`controller dsl 1, interface atm 1 (or controller t1 1)`

A 2MFT-T1/E1 is in slot 0, and a WIC-1SHDSL-V2 is in slot 1.	For 2MFT-T1/E1:
	`controller t1 0`
	`controller t1 1`
	For WIC-1SHDSL-V2:
	`controller dsl 2, interface atm 2(or controller t1 2)`

Interface Numbering on Cisco 2800 and Cisco 3800 Series Routers

This section describes the interface numbering scheme for Cisco 2800 and Cisco 3800 series routers If an interface card is installed in a Cisco 2800 series or Cisco 3800 series router, the interfaces must use a triple-number scheme to identify them. This triple-number assignment is different from the standard interface numbering scheme on other Cisco routers.

Table 37 shows the interface numbering for the onboard Fast Ethernet ports and the interface slots on Cisco 2800 and Cisco 3800 series routers.

Table 37 Interface Numbering on Cisco 2800 Series and Cisco 3800 Series Router

Port/Slot	Interface Numbering	Example
Fast Ethernet ports (onboard)	0/0, 0/1	FE 0/0, 0/1
Slot 1	Slot 0/0/0	FE 0/0/0, 0/0/1, 0/0/2, 0/0/3
Slot 2	Slot 0/1/0	(Serial 2T) Serial 0/1/0, 0/1/1
Slot 3	Slot 0/2/0	FE 0/2/0
Slot 4	Slot 0/3/0	(G.SHDSL) ATM 0/3/0

How to Configure ATM Mode for Two-Wire or Four-Wire SHDSL

To configure the ATM Mode for Two-Wire or Four-Wire SHDSL feature, perform the following tasks:

- Configuring G.SHDSL Service, page 636 (required)
- Verifying the ATM Configuration, page 642 (optional)
- Verifying DSL Configuration, page 646 (optional)
- Troubleshooting Tasks, page 651 (optional)

Configuring G.SHDSL Service

This section details how to configure the ATM Mode for Two-Wire or Four-Wire SHDSL feature for G.SHDSL service.

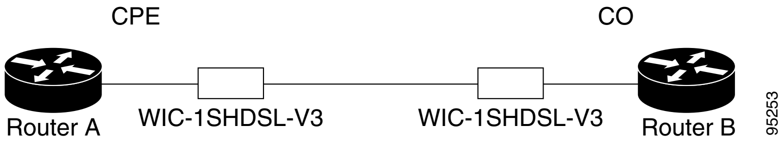
To configure G.SHDSL service in ATM mode on a Cisco router containing a G.SHDSL WIC, complete the steps in the Summary Steps or the Detailed Steps, beginning in global configuration mode.

Prerequisites

The following list of prerequisites should be followed for this configuration:

- A G.SHDSL WIC must be installed in the router to match the DSL service to be configured.
- Routers may be set up for back-to-back operation as shown in Figure 63 or they may be connected to a DSLAM.

Figure 63 Back-to-Back Setup



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller dsl** *slot*/*port*
4. **line-term** {**co** | **cpe**]
5. **dsl-mode shdsl symmetric annex** *mode*
6. **ignore-error-duration** *seconds*
7. **mode atm**
8. **line-mode** [**2-wire** | **4-wire** | **auto**]
9. **line-rate** [*rate* | **auto**]
10. **exit**
11. **interface atm** *slot*/*port*

12. **ip address** *IP-address subnet-mask*
13. **atm ilmi-keepalive** [*seconds*]
14. **pvc** [*name*] *vpi*/*vci*
15. **protocol** *protocol* [*protocol-address*]
16. **vbr-rt** *peak-rate average-cell-rate burst*
17. **encapsulation {aal2 | aal5ciscoppp | aal5mux | aal5nlpid | aal5snap | aal5autoppp}**
18. **exit**
19. **exit**
20. **exit**
21. **show interface atm** *slot*/*port*
22. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters the global configuration mode.

Step 3	`controller dsl` *`slot/port`*
	Example:
	`Router(config)# controller dsl 0/1`
		Enters controller configuration mode.
		The keywords and arguments are as follows:
		• **dsl**—The type of controller.
		• *slot/port*—The backplane slot number and port number for the interface being configured.

Step 4	`line-term {co | cpe]`
	Example:
	`Router(config-controller)# line-term cpe`
		Configures the DSL controller line termination as follows:
		• **co**—Central office.
		• **cpe**—Customer premises equipment.

	Command or Action	Purpose
Step 5	**dsl-mode shdsl symmetric annex** *mode* **Example:** `Router(config-controller)#` **`dsl-mode shdsl symmetric annex A`**	Sets the DSL operating mode parameters. The valid values are: • A: Supports Annex A of G.991.2 standard for North America. This is the default. • B: Supports Annex B of G.991.2 standard for Europe. • A–B: Supports Annex A or B. For CPE mode only. CO mode is not supported. Selected when the line trains. • A–B–ANFP: Supports Annex A or B–ANFP. For CPE mode only. CO mode is not supported. Selected when the line trains. • B–ANFP: Supports Annex B–ANFP.

Step 6	**ignore-error-duration** (*seconds*)
	Example:
	`Router(config-controller)#`
	`ignore-error-duration 15`
		(Optional) Permits the router to ignore errors for a given amount of time when training the line when connected to a controller with a different chipset type.
		• *seconds*—Number of seconds for which errors are ignored. The range is 15 to 30 seconds. If this value is omitted, an error message appears.

Step 7	**mode atm** **Example:** `Router(config-controller)#` **`mode atm`**	Enables ATM encapsulation and creates a logical ATM interface slot/port. **Note** If the **no mode atm** command is used to leave ATM mode, the router must be rebooted to clear the mode.

Step 8	**For CPE:**
	line-mode [**4-wire** | **2-wire** *line-number* | **auto**}
	For CO:
	line-mode {**4-wire** | **2-wire** *line-number*}
	Example:
	`Router(config-controller)#` **`line-mode 4-wire`**
		(Optional) Configures the controller to operate in two-wire or four-wire mode. The two-wire mode is the default if this step is not configured or if the mode is not specified.
		• **2-wire**—Configures the controller to operate in two-wire mode. This is the default if this step is omitted or if the mode is not specified.
		• **4-wire**—Configures the controller to operate in four-wire mode.
		• *line-number*—For two-wire mode only, selects the pair of wires used. Valid values are **line-zero** (default) or **line-one**. Line-zero selects RJ-11 pin 1 and pin 2; line-one selects RJ-11 pin 3 and pin 4.
		• **auto**—Configures the line mode to be automatically detected for the CPE. This option is not available for configuring the CO.

	Command or Action	Purpose

Step 9	**line-rate** {*rate* | **auto**}
	Example:
	`Router(config-controller)#` **`line-rate 1024`**
		Specifies the DSL line rate for the SHDSL port. Only fix line-rate mode is supported in four-wire mode. The argument is as follows:
		• auto—Allows the controller to select the rate. This option is available only in two-wire mode.
		• *rate*—Sets the DSL line rate. The supported line rates are as follows:
		– For two-wire mode—192, 256, 320, 384, 448, 512, 576, 640, 704, 768, 832, 896, 960, 1024, 1088, 1152, 1216, 1280, 1344, 1408, 1472, 1536, 1600, 1664, 1728, 1792, 1856, 1920, 1984, 2048, 2112, 2176, 2240, and 2304
		– For four-wire mode—384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1536, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2560, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608.
		Note The configured line rate is the data rate available. Third-party equipment may use a line rate that includes an additional SHDSL overhead of 8 kbps for two-wire mode or 16 kbps for four-wire mode.

Step 10	**exit** **Example:** `Router(config-controller)#` **`exit`**	Exits controller configuration mode.
Step 11	**interface atm** *slot*/*port* **Example:** `Router(config)#` **`interface atm 1/0`**	Enters ATM configuration mode for interface ATM 0 in slot 1. The keywords and arguments are as follows: • *slot*—The backplane slot number for the interface being configured. • *port*—The backplane port number for the interface being configured. **Note** If a slot has two subslots for WIC modules and no ATM interface is present in subslot 0, the WIC will take ATM x/0 as its interface number even if placed in subslot 1 (ATMx/1). If a two-port WIC is present in subslot 0, the WIC will use ATM x/2 as its interface number. This subslot number is pertinent to all interface commands such as **show interface atm** and **show dsl interface atm**.

	Command or Action	Purpose
Step 12	**ip address** *ip-address subnet-mask* **Example:** Router(config-if)# **ip address 192.168.10.25 255.255.255.0**	Assigns an IP address to the DSL ATM interface.
Step 13	**atm ilmi-keepalive** [*seconds*] **Example:** Router(config-if)# **atm ilmi-keepalive 5**	(Optional) Enables Integrated Local Management Interface (ILMI) keepalives. • *seconds*—The number of seconds between keepalives. • If you enable ILMI keepalives without specifying the seconds, the default time interval is 3 seconds.
Step 14	**pvc** [*name*] *vpi/vci* **Example:** Router(config-if)# **pvc [name] vpi/vci**	Enters atm-virtual-circuit (interface-atm-vc) configuration mode, and configures a new ATM permanent virtual circuit (PVC) by assigning a name (optional) and VPI/VCI numbers. The default traffic shaping is an unspecified bit rate (UBR); the default encapsulation is AAL5+LLC/SNAP. • *name*—(Optional) Name of the PVC or map. The name can be up to 15 characters long. • *vpi/*— ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a VPI value causes the VPI value to default to 0. Value Ranges: – Cisco 2600 and Cisco 3600 series routers using Inverse Multiplexing for ATM (IMA): 0 to 15, 64 to 79, 128 to 143, and 192 to 207 The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. • *vci*—ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atm vc-per-vp** command. Typically, lower values from 0 to 31 are reserved for specific traffic (for example, F4 OAM, SVC signaling, ILMI, and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.

	Command or Action	Purpose
Step 15	`protocol` *`protocol`* [*`protocol-address`*] **Example:** `Router(config-if-vc)# protocol ip 192.168.0.4`	(Optional) Enables IP connectivity and creates a point-to-point IP address for the virtual circuit (VC). • *protocol*—Choose the **ip** protocol for this configuration. • *protocol-address*—Destination address that is being mapped to a permanent virtual circuit (PVC).

Step 16	`vbr-rt` *`peak-rate average-cell-rate burst`*
	Example:
	`Router(config-if-vc)# vbr-rt peak-rate average-cell-rate burst`
		(Optional) Configures the PVC for real-time variable bit rate (VBR) traffic shaping.
		• *peak rate*—Peak cell rate (PCR).
		• *average-cell-rate*—Average cell rate (ACR).
		• *burst*—Burst size in cells.

Step 17	`encapsulation {aal2 | aal5ciscoppp | aal5mux | aal5nlpid | aal5snap | aal5autoppp}`
	Example:
	`Router(config-if-vc)# encapsulation aal2`
		(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type.
		• **aal2**—AAL2.
		• **aal5ciscoppp**—Cisco PPP over AAL5.
		• **aal5mux**—AAL5+MUX.
		• **aal5nlpid**—AAL5+NLPID.
		• **aal5snap**—AAL5+LLC/SNAP.
		• **aal5autoppp**—PPP Autosense over AAL5.
		The default is **aal5snap**.

Step 18	`exit`
	Example:
	`Router(config-if-vc)# exit`
		Exits interface-atm-vc configuration mode.

Step 19	`exit`
	Example:
	`Router(config-if)# exit`
		Exits ATM interface configuration mode.

Step 20	`exit`
	Example:
	`Router(config)# exit`
		Exits global configuration mode.

	Command or Action	Purpose
Step 21	**show interface atm** *slot***/***port* **Example:** `Router# show interface atm 1/0`	Displays the ATM interface configuration. The keywords and arguments are as follows: • *slot*—The backplane slot number for the interface being configured. • *port*—The backplane port number for the interface being configured.
Step 22	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Examples

Example of the Configuration Before Configuring ATM Mode:

```
controller DSL 0/0
 line-term cpe
```

Example for 4-wire ATM, Annex B, and Line Rate 3200

```
controller DSL 0/1
 mode atm
 line-term cpe
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 3200
```

What to Do Next

The next task is to verify the ATM mode or DSL mode for the router.

Verifying the ATM Configuration

Perform the steps in this section to verify the ATM Configuration.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show controllers atm** *slot*/*port*
4. **show atm vc**
5. **debug atm events**
6. **debug atm errors**
7. **show interface atm** *slot*/*port*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`show running-config`**
	Example:
	`Router# show running-config`
		Displays current running configuration and the status for all controllers.

Step 3	**`show controllers atm`** *`slot/port`*
	Example:
	`Router# show controllers atm 0/1`
		Displays ATM controller statistics.
		The keywords and arguments are as follows:
		• *slot*—The backplane slot number for the interface being configured.
		• *port*—The backplane port number for the interface being configured.

Step 4	**`show atm vc`**
	Example:
	`Router# show atm vc`
		Displays PVC status.

Step 5	**`debug atm events`**
	Example:
	`Router# debug atm events`
		Identifies ATM-related events as they are generated.

Step 6	**`debug atm errors`**
	Example:
	`Router# debug atm errors`
		Identifies interfaces with ATM errors.

Step 7	**`show interface atm`** *`slot/port`*
	Example:
	`Router# show interface atm 0/1`
		Displays the status of the ATM interface. Ensure that the ATM slot/port and the line protocol are up.
		The keywords and arguments are as follows:
		• *slot*—The backplane slot number for the interface being configured.
		• *port*—The backplane port number for the interface being configured.

Step 8	**`exit`**
	`Router# exit`
		Exits privileged EXEC mode.

Examples

The following example shows how the **show interface atm** command is used and that the ATM slot/port and line protocol are up:

```
Router#show interfaces atm 0/0

ATM0/0 is up, line protocol is up
  Hardware is DSLSAR
  MTU 4470 bytes, sub MTU 4470, BW 4608 Kbit, DLY 110 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Encapsulation(s): AAL5 , PVC mode
  23 maximum active VCs, 256 VCs per VP, 1 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  Last input 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
```

```
3725#show atm vc

           VCD /                                        Peak  Avg/Min
Burst
Interface  Name         VPI   VCI  Type   Encaps   SC   Kbps   Kbps
Cells  Sts
0/0.1      1              2   100  PVC    MUX      VBR    2000   2000 0   UP
0/1.1      1              2   100  PVC    SNAP     CBR    4608 UP
0/2.1      1              2   100  PVC    SNAP     VBR    4608   4200 0   UP
1/0.1      1              2   100  PVC    SNAP     VBR    4608   4608 0   UP
3725#

Router# show atm vc
            VCD /                                      Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells  Sts
1/0.3      2            9    36   PVC    MUX      UBR     800                UP
1/0.2      1            9    37   PVC    SNAP     UBR     800                UP
```

```
3725#show controllers atm 0/0

Interface: ATM0/0, Hardware: DSLSAR, State: up
IDB:     645F4B98  Instance: 645F646C  reg_dslsar:3C200000  wic_regs:
3C200080
PHY Inst:0         Ser0Inst: 645DFC8C  Ser1Inst:  645EA608  us_bwidth:4608
Slot:    0         Unit:     0         Subunit:   0         pkt Size: 4528
VCperVP: 256       max_vp:   256       max_vc:    65536     total vc: 1
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits: 8
vpvc_sel:3         enabled:  0         throttled: 0         cell drops: 0
Last Peridic Timer 00:44:26.872(2666872)
Parallel reads to TCQ:0  tx count reset = 0, periodic safe start = 0
Attempts to overwrite SCC txring: 0
Host Controller lockup recovery Info:
       recovery count1= 0, recovery count2= 0
Saved Host Controller Info to check any lockup:
      scc = 0, output_qcount = 0, head:0,
      buf addr = 0x00000000, serial outputs = 0
      scc = 1, output_qcount = 0, head:54,
      buf addr = 0x00000000, serial outputs = 212
```

```
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 0, current queue depth = 0, drops = 0, urun
cnt = 0, total cnt = 106
Serial idb tx count: AAL5: 0, RAW: 212, Drop count:AAL5: 0, RAW: 0
Host Controller Clock rate Info:
SCC Clockrates:
        SCC0 = 1000000 (ATM0/0)
        SCC1 = 8000000 (ATM0/0)
        SCC2 = 1000000 (ATM0/1)
        SCC3 = 1000000 (ATM0/2)
        SCC4 = 5300000 (ATM0/1)
        SCC5 = 8000000 (ATM0/2)
        SCC6 = 0
        SCC7 = 0

WIC    Register   Value      Notes
---------------   ---------- ----------
FPGA Dev ID (LB)  0x53       'S'
FPGA Dev ID (UB)  0x4E       'N'
FPGA Revision     0xA7
WIC Config Reg    0x35       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 0;
                             NTR Enable = 0;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad G.SHDSL ATM/T1/E1 access
Int 0 Enable Reg  0x01       G.SHDSL ATM/T1/E1 normal interrupt enabled
                             G.SHDSL ATM/T1/E1 error interrupt disabled

DSLSAR Register   Value      Notes
---------------   ---------- ----------
sdram_refresh:    0x410FFFF  Expected value: 0x428xxxx
intr_event_reg:   0xC0       TMR.
intr_enable_reg:  0x13C      FIFOF.FBQE.RQAF.RPQAF.TSQAF.
config:           0x660D0A20 UTOPIA.RXEN.RegulateXmit.RMCell.TXEN.
                             Rx Buffer size: 8192.  RCT: Large, VPI Bits:
8.
status:           0x0
clkPerCell:       814121   (line rate: 4608 Kbps)
Pre-timer Count:  461
rcid_tableBase:   0x0
rct_base:         0x10000
tstBase1:         0x13C28    TST boot jump.
rawCellBase:      0x14300    (0/128) slots used.
rpq_base:         0x16000
tsqb(Tx Stat Q):  0x17000
fbq_base:         0x17880    (fbq_count: 128)
txChanQueue:      0x18000
rxBuffers:        0x30000
txBuffers:        0x130000
Lookup Error cnt: 0x0
Invalid Cell cnt: 0x0
SCCA Rx Errors:   0x0
SCCB Rx Errors:   0x0
Drop Pkt Count:   0x0
Total Tx Count:   0x0
Total Rx Count:   0x0
Timer:            0x73A141
DSLSAR Interrupts:0x0
       Last Addr:0x12E14
```

```
Router# show controllers atm 1/0

Interface ATM1/0 is up
  Hardware is DSLSAR (with Globespan G.SHDSL Module)
IDB:    62586758  Instance:6258E054  reg_dslsar:3C810000  wic_regs:3C810080
PHY Inst:62588490  Ser0Inst:62573074  Ser1Inst: 6257CBD8  us_bwidth:800
Slot:   1         Unit:    1         Subunit:   0         pkt Size:4496
VCperVP:256       max_vp:  256       max_vc:    65536     total vc:2
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits:8
vpvc_sel:3         enabled: 0         throttled:0

WIC    Register   Value      Notes
---------------   ---------- ----------
WIC Config Reg    0x45       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 1;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad ADSL access
Int 0 Enable Reg  0x03       ADSL normal interrupt enabled
                             ADSL error interrupt enabled
```

What to Do Next

Verify the configuration using the detailed steps in the “Verifying DSL Configuration” section on page 646.

Verifying DSL Configuration

Perform the steps in this section to verify the DSL Configuration.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show controller dsl** *slot/port*
4. **debug xdsl application**
5. **debug xdsl eoc**
6. **debug xdsl error**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show running-config`
	Example:
	`Router# show running-config`
		Displays the current running configuration and the status for all controllers.

Step 3	**show controller dsl** *slot***/***port* **Example:** `Router# show controller dsl 0/2`	Displays the DSL controller status. The keywords and arguments are as follows: • *slot*—The backplane slot number for the interface being configured. • *port*—The backplane port number for the interface being configured.

Step 4	`debug xdsl application`
	Example:
	`Router# debug dsl application`
		Displays output of the DSL if the DSL does not come up.

Step 5	`debug xdsl eoc`
	Example:
	`Router# debug xdsl eoc`
		Displays what is in the Embedded Operation Channel (EOC) messages.

Step 6	`debug xdsl error`
	Example:
	`Router# debug xdsl error`
		Displays error messages.

Step 7	`exit`
	`Router# exit`
		Exits privileged EXEC mode.

Examples

The following example shows how to verify four-wire ATM mode in line zero (CPE):

```
Router#show controller dsl 0/0

DSL 0/0 controller UP
 SLOT 0: Globespan xDSL controller chipset
 DSL mode: SHDSL Annex B
 Frame mode: Utopia
 Configured Line rate: 4608Kbps
 Line Re-activated 4 times after system bootup
 LOSW Defect alarm: ACTIVE
 CRC per second alarm: ACTIVE
 Line termination: CPE
 FPGA Revision: 0xA7
```

```
Line 0 statistics

        Current 15 min CRC: 2116
        Current 15 min LOSW Defect: 8
        Current 15 min ES: 16
        Current 15 min SES: 15
        Current 15 min UAS: 112

        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0


Line 1 statistics

        Current 15 min CRC: 450
        Current 15 min LOSW Defect: 0
        Current 15 min ES: 6
        Current 15 min SES: 5
        Current 15 min UAS: 61

        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0

 Line-0 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  Data, Status 1
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.600 dB
 Transmit Power:  8.5 dB
 Receiver Gain:  19.5420 dB
 SNR Sampling:  37.9860 dB
 Line-1 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  Data, Status 1
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.4294966516 dB
 Transmit Power:  8.5 dB
 Receiver Gain:  19.5420 dB
 SNR Sampling:  37.6080 dB
 Dying Gasp: Present
```

Sample Output—Building Configuration

```
Router>show running-config

Current configuration : 3183 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3725
!
boot-start-marker
boot system flash c3725-is-mz.0424
boot system tftp shriv/c3725-is-mz.new 223.255.254.254
boot-end-marker
!
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
!
!
!
controller DSL 0/0
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 0/1
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
controller DSL 0/2
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 1/0
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
```

```
!
!
interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/0.1 point-to-point
 ip address 5.0.0.1 255.0.0.0
 pvc 2/100
  vbr-rt 2000 2000
  oam-pvc 0
  encapsulation aal5mux ip
 !
!
interface FastEthernet0/0
 ip address 1.3.208.25 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface ATM0/1
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
!
interface ATM0/1.1 point-to-point
 ip address 6.0.0.1 255.0.0.0
 pvc 2/100
  cbr 4608
 !
!
interface FastEthernet0/1
 mac-address 0000.0000.0011
 ip address 70.0.0.2 255.0.0.0 secondary
 ip address 90.0.0.2 255.0.0.0 secondary
 ip address 50.0.0.2 255.0.0.0
 load-interval 30
 speed 100
 full-duplex
 no cdp enable
!
interface ATM0/2
 no ip address
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/2.1 point-to-point
 ip address 7.0.0.1 255.0.0.0
 pvc 2/100
  vbr-nrt 4608 4200
 !
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
!
interface ATM1/0.1 point-to-point
 ip address 8.0.0.1 255.0.0.0
 pvc 2/100
```

```
  vbr-nrt 4608 4608
 !
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 172.19.163.44
ip classless
ip route 60.0.0.0 255.0.0.0 ATM1/0.1
ip route 80.0.0.0 255.0.0.0 ATM0/1.1
ip route 223.255.254.254 255.255.255.255 FastEthernet0/0
ip route 223.255.254.254 255.255.255.255 1.3.0.1
ip http server
!
!
access-list 101 permit ip host 20.0.0.2 host 20.0.0.1
snmp-server community public RO
snmp-server enable traps tty
no cdp run
!
!
!
control-plane
!
!
!
!
!
!
!
alias exec c conf t
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
!
end
```

Troubleshooting Tasks

The following commands verify hardware on the router:

- **show version**—Lists the modules installed in the router. If DSL controllers are installed, the output displays the following line:

- `1 DSL controller`—Indicates one DSL controller is installed in the router

and one of the following lines:

- `1 ATM network interface(s)`—If the DSL controller is configured for mode ATM
- `1 Channelized T1/PRI port(s)`—If the DSL controller is configured for mode T1

- **show controllers atm—**Displays the ATM controller status and statistics. The sample below shows the output in ATM mode. Actual output may vary depending on the router and the configuration.

```
Router# show controllers atm 0/0
Interface: ATM0/0, Hardware: DSLSAR, State: up
IDB:     645F4B98  Instance: 645F646C  reg_dslsar:3C200000  wic_regs: 3C200080
PHY Inst:0         Ser0Inst: 645DFC8C  Ser1Inst:  645EA608  us_bwidth:4608
Slot:    0         Unit:     0         Subunit:   0         pkt Size: 4528
VCperVP: 256       max_vp:   256       max_vc:    65536     total vc: 1
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits: 8
vpvc_sel:3         enabled:  0         throttled: 0         cell drops: 0
Last Peridic Timer 00:44:26.872(2666872)
Parallel reads to TCQ:0  tx count reset = 0, periodic safe start = 0
Attempts to overwrite SCC txring: 0
Host Controller lockup recovery Info:
       recovery count1= 0, recovery count2= 0
Saved Host Controller Info to check any lockup:
      scc = 0, output_qcount = 0, head:0,
      buf addr = 0x00000000, serial outputs = 0
      scc = 1, output_qcount = 0, head:54,
      buf addr = 0x00000000, serial outputs = 212
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 0, current queue depth = 0, drops = 0, urun
cnt = 0, total cnt = 106
Serial idb tx count: AAL5: 0, RAW: 212, Drop count:AAL5: 0, RAW: 0
Host Controller Clock rate Info:
SCC Clockrates:
        SCC0 = 1000000 (ATM0/0)
        SCC1 = 8000000 (ATM0/0)
        SCC2 = 1000000 (ATM0/1)
        SCC3 = 1000000 (ATM0/2)
        SCC4 = 5300000 (ATM0/1)
        SCC5 = 8000000 (ATM0/2)
        SCC6 = 0
        SCC7 = 0

WIC    Register   Value      Notes
---------------   ---------- ----------
FPGA Dev ID (LB)  0x53       'S'
FPGA Dev ID (UB)  0x4E       'N'
FPGA Revision     0xA7
WIC Config Reg    0x35       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 0;
                             NTR Enable = 0;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad G.SHDSL ATM/T1/E1 access
Int 0 Enable Reg  0x01       G.SHDSL ATM/T1/E1 normal interrupt enabled
                             G.SHDSL ATM/T1/E1 error interrupt disabled

DSLSAR Register   Value      Notes
---------------   ---------- ----------
sdram_refresh:    0x410FFFF  Expected value: 0x428xxxx
```

```
intr_event_reg:   0xC0       TMR.
intr_enable_reg:  0x13C      FIFOF.FBQE.RQAF.RPQAF.TSQAF.
config:           0x660D0A20 UTOPIA.RXEN.RegulateXmit.RMCell.TXEN.
                             Rx Buffer size: 8192.  RCT: Large, VPI Bits: 8.
status:           0x0
clkPerCell:       814121   (line rate: 4608 Kbps)
Pre-timer Count:  461
rcid_tableBase:   0x0
rct_base:         0x10000
tstBase1:         0x13C28    TST boot jump.
rawCellBase:      0x14300    (0/128) slots used.
rpq_base:         0x16000
tsqb(Tx Stat Q):  0x17000
fbq_base:         0x17880    (fbq_count: 128)
txChanQueue:      0x18000
rxBuffers:        0x30000
txBuffers:        0x130000
Lookup Error cnt: 0x0
Invalid Cell cnt: 0x0
SCCA Rx Errors:   0x0
SCCB Rx Errors:   0x0
Drop Pkt Count:   0x0
Total Tx Count:   0x0
Total Rx Count:   0x0
Timer:            0x73A141
DSLSAR Interrupts:0x0
       Last Addr:0x12E14
```

- **show controllers dsl**—Displays the DSL controller status and statistics. The sample below shows the output in T1 mode. Actual output may vary depending on the router and the configuration.

```
Router# show controllers dsl 0/0

 DSL 0/0 controller UP
 Globespan xDSL controller chipset
 DSL mode: SHDSL Annex B
 Frame mode: Utopia
 Configured Line rate: 4608Kbps
 Line Re-activated 5 times after system bootup
 LOSW Defect alarm: ACTIVE
 CRC per second alarm: ACTIVE
 Line termination: CO
 FPGA Revision: 0xA7

Line 0 statistics

        Current 15 min CRC: 679
        Current 15 min LOSW Defect: 8
        Current 15 min ES: 5
        Current 15 min SES: 5
        Current 15 min UAS: 441

        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0


Line 1 statistics

        Current 15 min CRC: 577
        Current 15 min LOSW Defect: 8
        Current 15 min ES: 7
        Current 15 min SES: 4
        Current 15 min UAS: 455

        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0

 Line-0 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  Data, Status 1
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.600 dB
 Transmit Power:  8.5 dB
 Receiver Gain:  21.420 dB
 SNR Sampling:  39.3690 dB
 Line-1 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  Data, Status 1
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.4294966256 dB
 Transmit Power:  8.5 dB
 Receiver Gain:  21.420 dB
 SNR Sampling:  39.1570 dB
 Dying Gasp: Present
```

- **debug xdsl application**—Displays output from the xDSL to see what is happening if the DSL does not come up. When using the debug xdsl application command, resources and the buffer are used and will impact operation.

```
Router# debug xdsl application
xDSL application debugging is on
Router#
Apr 23 06:01:26.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:27.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:27.720: DSL 0/0 process_get_wakeup
Apr 23 06:01:27.720: DSL 0/0 xdsl_process_boolean_events
XDSL_LINE_UP_EVENT:
Apr 23 06:01:28.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:29.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:30.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:31.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:32.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:33.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:34.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:34.476: DSL 0/0   SNR Sampling: 42.8370 dB
Apr 23 06:01:35.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:35.476: DSL 0/0   SNR Sampling: 41.9650 dB
Apr 23 06:01:36.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:36.476: DSL 0/0   SNR Sampling: 41.2400 dB
Apr 23 06:01:37.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:37.476: DSL 0/0   SNR Sampling: 40.6180 dB
Apr 23 06:01:37.476: DSL 0/0 xdsl_background_process: one_second_timer triggers
download
```

```
Apr 23 06:01:37.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:37.476: DSL 0/0 xdsl_background_process:Download boolean event received
Apr 23 06:01:37.476: DSL 0/0 xdsl_controller_reset: cdb-state=down
Apr 23 06:01:37.476: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to down
Apr 23 06:01:38.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:39.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:40.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:41.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:42.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:43.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:44.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:45.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:46.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:47.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:48.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:49.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:50.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:51.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:52.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:53.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:54.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:55.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:56.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.796: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.796: DSL 0/0 xdsl_process_boolean_events
XDSL_LINE_UP_EVENT:
Apr 23 06:01:57.812: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.812: DSL 0/0 xdsl_background_process: XDSL link up boolean event
received
Apr 23 06:01:57.812:  DSL 0/0 controller Link up! line rate: 4608 Kbps

Apr 23 06:01:57.812: DSL 0/0 xdsl_controller_reset: cdb-state=up
Apr 23 06:01:57.812: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
Apr 23 06:01:57.812: DSL 0/0
Apr 23 06:01:57.812:  Dslsar data rate 4608
Apr 23 06:01:57.816: DSL 0/0 TipRing 1, Xmit_Power Val 85, xmit_power 8.5
Apr 23 06:01:57.816: DSL 0/0 Mode 2, BW 4608, power_base_value 145, power_backoff 6
Apr 23 06:01:57.912: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.916: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.916: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.008: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.008: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.012: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.012: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.104: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.104: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.108: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.108: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.200: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.204: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.204: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.204: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.208: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.296: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.392: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:59.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:00.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:01.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:02.476: DSL 0/0 process_get_wakeup
Router#
Router#
Apr 23 06:02:02.920: DSL 0/0 process_get_wakeup
Apr 23 06:02:02.920: DSL 0/0 process_get_wakeup
Apr 23 06:02:02.920: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:03.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.016: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:03.020: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.112: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.208: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.304: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.476: DSL 0/0 process_get_wakeup
Router#
Router#
Apr 23 06:02:04.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:04.476: DSL 0/0   SNR Sampling: 42.3790 dB
Apr 23 06:02:04.476: DSL 0/0   SNR Sampling: 42.8370 dB
Router#
Apr 23 06:02:04.476: %LINK-3-UPDOWN: Interface ATM0/0, changed state to up
Apr 23 06:02:05.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:05.476: DSL 0/0   SNR Sampling: 41.5880 dB
Apr 23 06:02:05.476: DSL 0/0   SNR Sampling: 42.3790 dB
Apr 23 06:02:05.476: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, changed
state to up
Router#
Router#
Apr 23 06:02:06.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:06.476: DSL 0/0   SNR Sampling: 40.9180 dB
Apr 23 06:02:06.476: DSL 0/0   SNR Sampling: 41.5880 dB
Apr 23 06:02:07.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:07.476: DSL 0/0   SNR Sampling: 40.6180 dB
Apr 23 06:02:07.476: DSL 0/0   SNR Sampling: 41.2400 dBu all
Apr 23 06:02:07.912: DSL 0/0 process_get_wakeup
Apr 23 06:02:07.912: DSL 0/0 process_get_wakeup
Apr 23 06:02:07.912: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:08.008: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.008: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.008: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.008: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:08.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.104: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.200: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.296: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.476: DSL 0/0
All possible debugging has been turned off
Router#
Router#
Router#
Router#  SNR Sampling: 40.750 dB
Apr 23 06:02:08.476: DSL 0/0   SNR Sampling: 40.6180 dB
Apr 23 06:02:09.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:09.476: DSL 0/0   SNR Sampling: 39.5920 dB
Apr 23 06:02:09.476: DSL 0/0   SNR Sampling: 40.3380 dB
```

- **debug xdsl driver**—Displays what is happening when downloading and installing the drivers. The following example displays a sample output from the **debug xdsl driver** command:
  - 4-wire mode:

    ```
    Router# debug xdsl driver

    xDSL driver debugging is on
    Router#
    ```

```
01:04:18: DSL 2/0 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2 framer intr_status 0xC4
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 2/0 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/1 framer intr_status 0xC1
01:04:18: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 2/0 framer intr_status 0xC4
01:04:18: DSL 2/0 framer intr_status 0xC1
01:04:18: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2 framer intr_status 0xC4
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2
01:04:18: DSL 0/2 framer intr_status 0xC1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2 framer intr_status 0xC4
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/1 framer intr_status 0xC1
01:04:19: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 2/0 framer intr_status 0xC1
01:04:19: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/2 framer intr_status 0xC1
01:04:19: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/1 framer intr_status 0xC1
01:04:19: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 2/0 framer intr_status 0xC1
01:04:19: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/2 framer intr_status 0xC1
01:04:19: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/1 framer intr_status 0xC1
01:04:19: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 2/0 framer intr_status 0xC1
01:04:19: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/2 framer intr_status 0xC1
01:04:19: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:22: DSL 0/0  dsp interrupt-download next block for line-0
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:22: DSL 0/0  dsp interrupt-download next block for line-1
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:22: DSL 0/0  dsp interrupt-download next block for line-0
```

```
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:22: DSL 0/0  dsp interrupt-download next block for line-1
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:23: DSL 0/0  dsp interrupt-download next block for line-0
01:04:23: DSL 0/0 DSP interrupt disabled
01:04:23: DSL 0/0  Download completed for line-0
01:04:23: DSL 0/0 framer intr_status 0xC0
01:04:23: DSL 0/0  dsp interrupt-download next block for line-1
01:04:23: DSL 0/0 DSP interrupt disabled
01:04:23: DSL 0/0  Download completed for line-1
01:04:23: DSL 0/0 Framer interrupt enabled
01:04:23: DSL 0/0 framer intr_status 0xC0
01:04:23:  DSL 0/0 controller Link up! line rate: 4608 Kbps

01:04:23: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
01:04:23: DSL 0/0 framer intr_status 0xC4
01:04:23: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
01:04:23: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
01:04:23: DSL 0/0 framer intr_status 0xC1
01:04:23: DSL 0/0 framer intr_status 0xC4
```

- 2-wire mode line-zero:

```
Router# debug xdsl driver
xDSL driver debugging is on

00:58:22: DSL 0/0  dsp interrupt-download next block for line-0
00:58:23: DSL 0/0 framer intr_status 0xC0
00:58:24: DSL 0/0  dsp interrupt-download next block for line-0
00:58:24: DSL 0/0 framer intr_status 0xC0
00:58:37: DSL 0/0  dsp interrupt-download next block for line-0
00:58:37: DSL 0/0 framer intr_status 0xC0
00:58:38: DSL 0/0  dsp interrupt-download next block for line-0
00:58:38: DSL 0/0 framer intr_status 0xC0
00:58:38: DSL 0/0  dsp interrupt-download next block for line-0
00:58:38: DSL 0/0 DSP interrupt disabled
00:58:38: DSL 0/0  Download completed for line-0
00:58:38: DSL 0/0 Framer interrupt enabled
00:58:38: DSL 0/0 framer intr_status 0xC0
00:58:38:  DSL 0/0 controller Link up! line rate: 1600 Kbps

00:58:38: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
00:58:38:  Dslsar data rate 1600
00:58:38: DSL 0/0 framer intr_status 0xC4
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC4
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC1
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC4
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC1
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
```

- 2-wire mode line-one:

```
Router# debug xdsl driver
xDSL driver debugging is on
```

```
00:55:15: DSL 0/0  dsp interrupt-download next block for line-1
00:55:15: DSL 0/0 framer intr_status 0xC0
00:55:16: DSL 0/0  dsp interrupt-download next block for line-1
00:55:16: DSL 0/0 framer intr_status 0xC0
00:55:17: DSL 0/0  dsp interrupt-download next block for line-1
00:55:17: DSL 0/0 framer intr_status 0xC0
00:55:19: DSL 0/0  dsp interrupt-download next block for line-1
00:55:19: DSL 0/0 framer intr_status 0xC0
00:55:32: DSL 0/0  dsp interrupt-download next block for line-1
00:55:32: DSL 0/0 framer intr_status 0xC0
00:55:32: DSL 0/0  dsp interrupt-download next block for line-1
00:55:32: DSL 0/0 framer intr_status 0xC0
00:55:32: DSL 0/0  dsp interrupt-download next block for line-1
00:55:32: DSL 0/0 DSP interrupt disabled
00:55:32: DSL 0/0  Download completed for line-1
00:55:32: DSL 0/0 Framer interrupt enabled
00:55:32: DSL 0/0 framer intr_status 0xC0
00:55:32:  DSL 0/0 controller Link up! line rate: 1600 Kbps

00:55:32: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
00:55:32:  Dslsar data rate 1600
00:55:46: %LINK-3-UPDOWN: Interface ATM0/0, changed state to up
00:55:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, changed state to
up
00:56:28: DSL 0/0 framer intr_status 0xC8
00:56:28: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:28: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:28: DSL 0/0 framer intr_status 0xC8
00:56:28: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:28: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:28: DSL 0/0 framer intr_status 0xC2
00:56:28: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:28: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0 framer intr_status 0xC8
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:33: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0 framer intr_status 0xC2
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:33: DSL 0/0
00:56:33: DSL 0/0 framer intr_status 0xC8  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:33: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0 framer intr_status 0xC8
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
```

- **debug xdsl eoc**—Displays what is in the embedded operations channel messages. The following example shows the use of the **debug xdsl eoc** command, sample output, and use of the command to stop the display.

```
Router# debug xdsl eoc

xDSL EOC debugging is on
Router#
Apr 23 07:31:26.945:  DSL 0/0 controller Link up! line rate: 4608 Kbps

Apr 23 07:31:26.945: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
Apr 23 07:31:27.057: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
Apr 23 07:31:27.057: DSL 0/0:Current length 40 GTI_OK
Apr 23 07:31:27.057: DSL 0/0:msg rcvd line 0
Apr 23 07:31:27.057: DSL 0/0: GT_FAIL
Apr 23 07:31:27.057:   eoc_get_message for line::0
Apr 23 07:31:27.057:  Rx EOC remove transparency:: 1F 1  0  46 10
Apr 23 07:31:27.057: data_transparency_remove: Done, eoc packet size = 5
Apr 23 07:31:27.057:   Good eoc packet received
Apr 23 07:31:27.057:  incoming request eocmsgid: 1 from line 0
Apr 23 07:31:27.057:  Tx Converted EOC message:: 21 81 1  43 43 49 53 43
4F 0  0  0  2  1  0  E9 61
Apr 23 07:31:27.057: data_transparency_add: eoc packet size - before 17, after 17

Apr 23 07:31:27.153: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
Apr 23 07:31:27.153: DSL 0/0:Current length 40 GTI_OK
Apr 23 07:31:27.153: DSL 0/0:msg rcvd line 0
Apr 23 07:31:27.153: DSL 0/0: GT_FAIL
Apr 23 07:31:27.153:   eoc_get_message for line::0
Apr 23 07:31:27.153:  Rx EOC remove transparency:: 12 2  74 8A
Apr 23 07:31:27.153: data_transparency_remove: Done, eoc packet size = 4

Apr 23 07:31:27.153:   Good eoc packet received
Apr 23 07:31:27.153:  incoming request eocmsgid: 2 from line 0
Apr 23 07:31:27.153:  Tx Converted EOC message:: 21 82 1  0  0  0  0  0
41 32 39 37 33 33 43 4E 53 38 44 44 30 41 41 41 43 43 49 53 43 4F 0  0  0
43 53 43 4F 2D 31 53 48 44 53 4C 0  46 4F 43 30 37 34 32 31 54 41 31 0  31
32 2E 33 28 32 30 30 34 30 33 0  60 F0
Apr 23 07:31:27.153: data_transparency_add: eoc packet size - before 71, after 71

Apr 23 07:31:27.249: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
Apr 23 07:31:27.249: DSL 0/0:Current length 40 GTI_OK
Apr 23 07:31:27.249: DSL 0/0:msg rcvd line 0
Apr 23 07:31:27.249: DSL 0/0: GT_FAIL
Apr 23 07:31:27.249:   eoc_get_message for line::0
Apr 23 07:31:27.249:  Rx EOC remove transparency:: 12 3  0  0  6D E9
Apr 23 07:31:27.249: data_transparency_remove: Done, eoc packet size = 6

Apr 23 07:31:27.249:   Good eoc packet received
Apr 23 07:31:27.249:  incoming request eocmsgid: 3 from line 0
Apr 23 07:31:27.249:  Tx Converted EOC message:: 21 83 0  0  0  1  AC
Apr 23 07:31:27.249: data_transparency_add: eoc packet size - before 7, after 7
GSI Tx buffer yet to transmit

Apr 23 07:31:27.345: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
Apr 23 07:31:27.345: DSL 0/0:Current length 40 GTI_OK
Apr 23 07:31:27.345: DSL 0/0:msg rcvd line 0
Apr 23 07:31:27.345: DSL 0/0: GT_FAIL
Apr 23 07:31:27.345:   eoc_get_message for line::0
Apr 23 07:31:27.345:  Rx EOC remove transparency:: 12 5  0  0  0  E9 0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  32 42
Apr 23 07:31:27.345: data_transparency_remove: Done, eoc packet size = 24

Apr 23 07:31:27.345:   Good eoc packet received
Apr 23 07:31:27.345:  incoming request eocmsgid: 5 from line 0
Apr 23 07:31:27.345:  Tx Converted EOC message:: 21 85 0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  1E AB
Apr 23 07:31:27.345: data_transparency_add: eoc packet size - before 26,
after 26
GSI Tx buffer yet to transmit

Apr 23 07:31:27.349: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
Apr 23 07:31:27.349: DSL 0/0: Current length 40 GTI_EOM
Apr 23 07:31:27.349: DSL 0/0: GT_FAIL
Apr 23 07:31:32.049: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
Apr 23 07:31:32.049: DSL 0/0:Current length 40 GTI_OK
Apr 23 07:31:32.049: DSL 0/0:msg rcvd line 0
Apr 23 07:31:32.049: DSL 0/0: GT_FAIL
Apr 23 07:31:32.049:   eoc_get_message for line::0
Apr 23 07:31:32.049:  Rx EOC remove transparency:: 12 C  A  63
Apr 23 07:31:32.049: data_transparency_remove: Done, eoc packet size = 4
Apr 23 07:31:32.049:   Good eoc packet received
Apr 23 07:31:32.049:  incoming request eocmsgid: 12 from line 0
Apr 23 07:31:32.049:  Tx Converted EOC message:: 21 8C 0  9  0  5  5  2
A2 2  30 6  1  EB F2
Apr 23 07:31:32.049: data_transparency_add: eoc packet size - before 15, after 15

Apr 23 07:31:32.049:  size of eoc status response :: 13
Apr 23 07:31:32.049:  Tx Converted EOC message:: 21 8C 0  0  0  4  4  2  8
1  2C 6  2  83 38
Apr 23 07:31:32.049: data_transparency_add: eoc packet size - before 15, after 15

Apr 23 07:31:32.049:  size of eoc status response :: 13
Apr 23 07:31:32.049:  Tx Converted EOC message:: 21 89 5  52 93
Apr 23 07:31:32.049: data_transparency_add: eoc packet size - before 5, after 5
```

- **debug xdsl error**—Displays error messages. The following example shows the **debug xdsl error** command.

```
Router# debug xdsl error
xDSL error debugging is on
Router#
```

Configuration Examples for ATM Mode for Two-Wire or Four-Wire SHDSL

The following are configuration examples for the ATM Mode for Two-Wire or Four-Wire SHDSL feature:

- Router A: CPE Configuration Example
- Router B: CO Configuration Example

Router A: CPE Configuration Example

```
controller DSL 1/2
 mode atm
 line-term cpe
 line-mode 2-wire line-zero
 dsl-mode shdsl symmetric annex B
!
!
!
!
connect hp DSL 1/0 0 DSL 1/2 0
!
!
```

Router B: CO Configuration Example

```
Current configuration : 3183 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname 3725
!
boot-start-marker
boot system flash c3725-is-mz.0424
boot system tftp shriv/c3725-is-mz.new 223.255.254.254
boot-end-marker
!
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
!
!
!
controller DSL 0/0
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 0/1
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
controller DSL 0/2
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 1/0
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
!
!
interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/0.1 point-to-point
```

```
 ip address 5.0.0.1 255.0.0.0
 pvc 2/100
  vbr-rt 2000 2000
  oam-pvc 0
  encapsulation aal5mux ip
 !
!
interface FastEthernet0/0
 ip address 1.3.208.25 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface ATM0/1
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
!
interface ATM0/1.1 point-to-point
 ip address 6.0.0.1 255.0.0.0
 pvc 2/100
  cbr 4608
 !
!
interface FastEthernet0/1
 mac-address 0000.0000.0011
 ip address 70.0.0.2 255.0.0.0 secondary
 ip address 90.0.0.2 255.0.0.0 secondary
 ip address 50.0.0.2 255.0.0.0
 load-interval 30
 speed 100
 full-duplex
 no cdp enable
!
interface ATM0/2
 no ip address
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/2.1 point-to-point
 ip address 7.0.0.1 255.0.0.0
 pvc 2/100
  vbr-nrt 4608 4200
 !
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
!
interface ATM1/0.1 point-to-point
 ip address 8.0.0.1 255.0.0.0
 pvc 2/100
  vbr-nrt 4608 4608
 !
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
```

```
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 172.19.163.44
ip classless
ip route 60.0.0.0 255.0.0.0 ATM1/0.1
ip route 80.0.0.0 255.0.0.0 ATM0/1.1
ip route 223.255.254.254 255.255.255.255 FastEthernet0/0
ip route 223.255.254.254 255.255.255.255 1.3.0.1
ip http server
!
!
access-list 101 permit ip host 20.0.0.2 host 20.0.0.1
snmp-server community public RO
snmp-server enable traps tty
no cdp run
!
!
!
control-plane
!
!
!
!
!
!
!
alias exec c conf t
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
!
end
```

Additional References

For additional information related to the ATM Mode for Two-Wire or Four-Wire SHDSL feature, refer to the following references.

Related Documents

Related Topic	Document Title
1-port G.SHDSL WAN interface card	*1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers*, Release 12.2(8)T
Voice configuration	*Cisco IOS Voice Configuration Library,* Release 12.3
Voice commands	*Cisco IOS Voice Command Reference,* Release 12.3
IP configuration	*Cisco IOS IP Configuration Guide*, Release 12.3
ATM configuration	*"Configuring ATM"* in the *Wide-Area Networking Configuration Guide*, Release 12.3
Voice over ATM with AAL5 and AAL2 support	*Voice over ATM*, Release 12.3

Standards

Standards	Title
ITU-T G.991.2 (SHDSL)	*Single-pair High-speed Digital Subscriber Line (SHDSL) Transceivers*
ITU-T G.994.1 (G.HDSL)	*Handshake Procedures for Digital Subscriber Line (DSL) Transceivers*

MIBs

MIBs	MIBs Link
• ATM MIB • HDSL2-SHDSL-LINE-MIB(RFC3276) • G.SHDSL MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this 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 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.

Modified Commands

- **controller dsl**
- **dsl-mode shdsl symmetric annex**
- **ignore-error-duration**
- **line-modeline-mode**
- **line-rate**
- **line-term**
- **loopback (DSL controller)**
- **show controller dsl**
- **snr margin**
- **debug xdsl application**
- **debug xdsl driver**
- **debug xdsl eoc**
- **debug xdsl error**

Glossary

ABR—available bit rate. An ATM service type in which the ATM network makes a “best effort” to meet the transmitter’s bandwidth requirements. ABR uses a congestion feedback mechanism that allows the ATM network to notify the transmitters that they should reduce their rate of data transmission until the congestion decreases. Thus, ABR offers a qualitative guarantee that the transmitter’s data can get to the intended receivers without unwanted cell loss.

ATM—Asynchronous Transfer Mode. A form of digitized data transmission based on fixed-length cells that can carry data, voice, and video at high speeds.

CBR—constant bit rate. A data transmission that can be represented by a nonvarying, or continuous, stream of bits or cell payloads. Applications such as voice circuits generate CBR traffic patterns. CBR is an ATM service type in which the ATM network guarantees to meet the transmitter’s bandwidth and quality-of-service (QoS) requirements.

CO—central office. Local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occur.

CPE—customer premises equipment. CPE includes devices, such as CSU/DSUs, modems, and ISDN terminal adapters, required to provide an electromagnetic termination for wide-area network circuits before connecting to the router or access server. This equipment was historically provided by the telephone company, but is now typically provided by the customer in North American markets.

Downstream—Refers to the transmission of data from the central office (CO or COE) to the customer premises equipment (CPE).

G.SHDSL—Multirate Symmetrical High-Speed Digital Subscriber Line.

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 (available bit rate), CBR, and VBR.

Upstream—Refers to the transmission of data from the customer premises equipment (CPE) to the central office equipment (CO or COE).

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—VBR-real-time is used for connections in which there is a fixed timing relationship between samples.

VBR-nrt—VBR-non-real-time 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.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.

APS Support on Cisco AS5850 STM-1 Interfaces

This feature provides SONET automatic protection switching (APS) on Cisco AS5850 STM-1 interfaces. SONET APS—also referred to as SDH multiplex section protection (MSP)—refers to the mechanism of providing fault tolerance through fiber cable redundancy in SONET/SDH networks. When the working fiber fails, the protect fiber quickly assumes its traffic load. Some command-line interface (CLI) commands are available to provide a measure of manual intervention in the APS switching process.

Feature History for the APS Support on Cisco AS5850 STM-1 Interfaces Feature

Release	Modification
12.3(11)T	This feature was introduced on the Cisco AS5850.

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 APS Support on Cisco AS5850 STM-1 Interfaces

This feature assumes familiarity with the ITU-T G.841 *Types and characteristics of SDH network protection architectures* standard.

Information About APS Support on Cisco AS5850 STM-1 Interfaces

To configure SONET APS on the STM-1 card, you should understand the following concepts.

- SONET APS Using an STM-1 Card, page 670
- Benefits of SONET APS Using an STM-1 Card, page 670

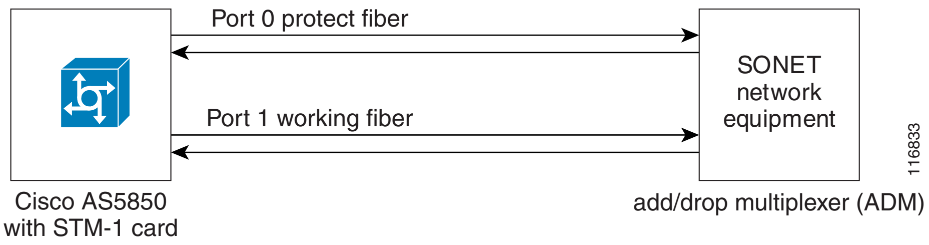
SONET APS Using an STM-1 Card

SONET APS provides the ability to switch fiber cable interfaces—referred to in this feature as ports—on an STM-1 card in a Cisco AS5850. The ability to switch from one SONET port to another SONET port in response to a fiber cut or module failure, signal failure, signal degradation, or manual intervention provides redundancy.

The protection mechanism used for this feature has a linear 1+1 architecture as described in the ITU-T G.841 standard and the Bellcore publication *GR-253-CORE, SONET Transport Systems; Common Generic Criteria, Section 5.3*. The connection may be bidirectional or unidirectional.

In the 1+1 architecture, a protect port is paired with each working port. Normally, the protect and working ports are connected to a SONET ADM (add/drop multiplexer), which sends the same signal payload to the working and protect ports. Figure 64 shows an APS configuration with the working and protect fibers terminating in SONET ports on the STM-1 card in a Cisco AS5850.

Figure 64 APS Configuration



When SONET APS is configured and a failure is detected on the working fiber, or when switch commands are entered through the command-line interface (CLI), the software switches the traffic to the protect fiber. The software also monitors the health of the protect fiber when APS is enabled and informs the user of any problems. When the protect fiber problem is resolved, normal APS operation is resumed.

Benefits of SONET APS Using an STM-1 Card

The STM-1 card is generally deployed by medium to large service providers who have a need for a larger DS0 capacity. The main benefits of using the STM-1 card over E1 interfaces are an initial lower cost of deployment compared to deploying 63 E1 interfaces, a lower recurring monthly charge, and lower maintenance cost because only one cable is required between the Main Distribution Facility (MDF) and the Cisco AS5850 instead of 63 cables. Service providers who carry voice data do expect to have more protection on an STM-1 port than on an E1 port because the STM-1 port supports a high density of DS0s

(1953). Network reliability could be severely impacted if 1953 connections are lost at the same time. SONET APS can provide the fiber protection and network resiliency expected by the service providers. The existing media gateways that support STM-1 already provide APS protection.

How to Configure APS Support on Cisco AS5850 STM-1 Interfaces

This section contains the following tasks:

- Configuring APS Support on the Cisco AS5850, page 671 (required)
- Issuing APS Switch Commands Using CLI, page 673 (optional)

Configuring APS Support on the Cisco AS5850

Perform this task to enable and configure APS on SONET ports on an STM-1 trunk card.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller sonet** *slot*/*port*
4. **main-fiber port** {**0** | **1**}
5. **aps protect**
6. **b2 sd-ber** *rate*
7. **b2 sf-ber** *rate*
8. **aps unidirectional**
9. **end**
10. **show controllers sonet** *slot*/*port*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**controller sonet** *slot***/***port* **Example:** `Router(config)# controller sonet 1/0`	Configures a SONET controller and enters controller configuration mode. • Use the *slot* argument to specify the slot number in which the STM-1 card resides. • The *port* argument is always 0 because only one port on the STM-1 card can be configured.

Step 4	**main-fiber port** {**0** | **1**}
	Example:
	`Router(config-controller)# main-fiber port 1`
		(Optional) Specifies the working port to use for the optical link connection on the SDH/STM-1 trunk card on a Cisco AS5850. The default is port 0.
		• We recommend that port 1 be configured as the working port.
		• The other port on the STM-1 card is configured automatically as the protect port when APS is enabled.
		• After APS is enabled, you cannot change the main-fiber (working) port until you disable APS.

Step 5	**aps protect** **Example:** `Router(config-controller)# aps protect`	Enables APS on the current working SONET port. • By default, the bidirectional mode is enabled.
Step 6	**b2 sd-ber** *rate* **Example:** `Router(config-controller)# b2 sd-ber 7`	Sets the signal degrade bit error rate (BER) threshold values. • Use this command to configure the threshold for degradation of quality of signal with b2 errors. • The rate value can be in the range from 3 to 9. A higher number represents better quality, and a value of 3 represents lower quality.
Step 7	**b2 sf-ber** *rate* **Example:** `Router(config-controller)# b2 sf-ber 4`	Sets the signal failure BER threshold values. • Use this command to configure the threshold for failure of quality of signal with b2 errors. • The rate value can be in the range from 3 to 9. A higher number represents better quality, and a value of 3 represents lower quality.
Step 8	**aps unidirectional** **Example:** `Router(config-controller)# aps unidirectional`	Configures APS to operate in unidirectional mode. • To return to bidirectional mode, use the **no** form of this command.

	Command or Action	Purpose

Step 9	**`end`**
	Example:
	`Router(config-controller)# end`
		Exits controller configuration mode and returns to privileged EXEC mode.

Step 10	**`show controllers sonet`** *`slot`*`/`*`port`*
	Example:
	`Router# show controllers sonet 1/0`
		Displays information about SONET controllers.
		• Only partial syntax is displayed here. For more details, see the **show controllers sonet** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.3 T.

Examples

The following example shows partial output from the **show controllers sonet** command.

```
Router# show controllers sonet 1/0

SONET 1/0 is up.
  Applique type is Channelized Sonet/SDH
  Clock Source is Line, AUG mapping is AU4.
  MSP 1+1 bi-directional enabled
  Protection fiber (Port 0), No Alarm, traffic in-use
  Working fiber (Port 1), No Alarm, traffic not in-use
  Local request: No Request
  Remote request: No Request

Medium info:
  Type: SDH, Line Coding: NRZ, Line Type: Short SM
.
.
.
```

Troubleshooting Tips

- Use the **show controllers sonet** command and look for any alarms or local and remote request information.
- Check that the ADM is sourcing the SONET clocking.

Issuing APS Switch Commands Using CLI

Perform this task to issue one or more of the optional APS switch commands when the working fiber is active but you want to switch to the protect fiber. The APS switch commands allow a measure of manual intervention in the APS process.

APS Switching Priority Levels

Each APS switch command has a priority level compared to the other APS switch commands and the signal status of the working and protect fibers. Table 38 shows the priority requests from the highest (lockout) to the lowest (manual). The actual decision-based activity performed by the software is quite complex; details are provided in the ITU-T G.841 *Types and characteristics of SDH network protection architectures* standard.

Table 38 APS Priority Request

Priority	Priority Request
1	Lockout of protect port
2	Forced switch
3	Signal failure—low priority
4	Signal degradation—low priority
5	Manual switch

SUMMARY STEPS

1. **enable**
2. **aps manual sonet** *slot*/*port* **from** {**protection** | **working**}
3. **aps force sonet** *slot*/*port* **from** {**protection** | **working**}
4. **aps lockout sonet** *slot*/*port*
5. **aps clear sonet** *slot*/*port*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`aps manual sonet`** *`slot`*/*`port`* **`from`** {**`protection`** | **`working`**}
	
	Example:
	`Router# aps manual sonet 1/0 from working`
		(Optional) Issues an APS manual request to switch from one port to the alternate port.
		• Use the **from protection** keywords to switch from the active protect fiber to the working fiber unless an equal or higher switching priority exists.
		• Use the **from working** keywords to switch from the active working fiber to the protect fiber unless an equal or higher switching priority exists.

Step 3	**`aps force sonet`** *`slot`*/*`port`* **`from`** {**`protection`** | **`working`**}
	
	Example:
	`Router# aps force sonet 1/0 from working`
		(Optional) Issues an APS force request to switch from one port to the alternate port.
		• Use the **from protection** keywords to switch from the active protect fiber to the working fiber unless an equal or higher switching priority exists.
		• Use the **from working** keywords to switch from the active working fiber to the protect fiber unless an equal or higher switching priority exists.

	Command or Action	Purpose

Step 4	**`aps lockout sonet`** *`slot/port`*
	Example:
	`Router# aps lockout sonet 1/0`
		(Optional) Issues an APS lockout of protection request.
		• Use this command to deny the working fiber access to the protect fiber unless an equal switching priority exists.
		• Lockout is defined as the highest APS request priority level.
		• If the protect fiber is active, this command switches the traffic to the working fiber.

Step 5	**`aps clear sonet`** *`slot/port`*
	Example:
	`Router# aps clear sonet 1/0`
		(Optional) Removes any APS priority requests configured for the specified port using the **aps lockout sonet**, **aps force sonet**, or **aps manual sonet** commands.

Configuration Examples for APS Support on Cisco AS5850 STM-1 Interfaces

This section contains the following configuration example:

- Configuring APS Support and APS Switch Commands on the Cisco AS5850: Example, page 675

Configuring APS Support and APS Switch Commands on the Cisco AS5850: Example

In the following example, SONET APS parameters are configured, and APS is enabled on port 1 of an STM-1 card in a Cisco AS5850. A manual APS switching request is configured, and partial output for the **show controllers sonet** command is displayed.

```
Router# configure terminal
Router (config)# controller sonet 1/0
Router (config-controller)# main-fiber port 1
Router (config-controller)# aps protect
Router (config-controller)# b2 sd-ber 7
Router (config-controller)# b2 sf-ber 4
Router (config-controller)# aps unidirectional
Router (config-controller)# end
Router# aps manual sonet 1/0 from working
```

```
Router# show controllers sonet

SONET 1/0 is up.
  Applique type is Channelized Sonet/SDH
  Clock Source is Line, AUG mapping is AU4.
  MSP 1+1 bi-directional enabled
  Protection fiber (Port 0), No Alarm, traffic in-use
  Working fiber (Port 1), No Alarm, traffic not in-use
  Local request: Manual Switch/Working
  Remote request: No request
.
.
.
```

Where to Go Next

For more details about the Cisco AS5850, visit the Cisco AS5850 Universal Gateway Introduction page under the Products and Service section on www.cisco.com.

Additional References

The following sections provide references related to the APS Support on Cisco AS5850 STM-1 Interfaces feature.

Related Documents

Related Topic	Document Title
Hardware and configuration information for the SDH/STM-1 trunk card	The “ SDH/STM-1 Trunk Card” chapter of the *Cisco AS5850 Universal Gateway Card Guide*
APS and SONET commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Interface and Hardware Component Command Reference*, Release 12.3 T
APS and SONET configuration	*Cisco IOS Interface and Hardware Component Configuration Guide*, Release 12.3

Standards

Standards	Title
Bellcore SONET linear 1+1 architecture	*GR-253-CORE, SONET Transport Systems; Common Generic Criteria, Section 5.3*
ITU-T G.841	*Types and characteristics of SDH network protection architectures*

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.	—

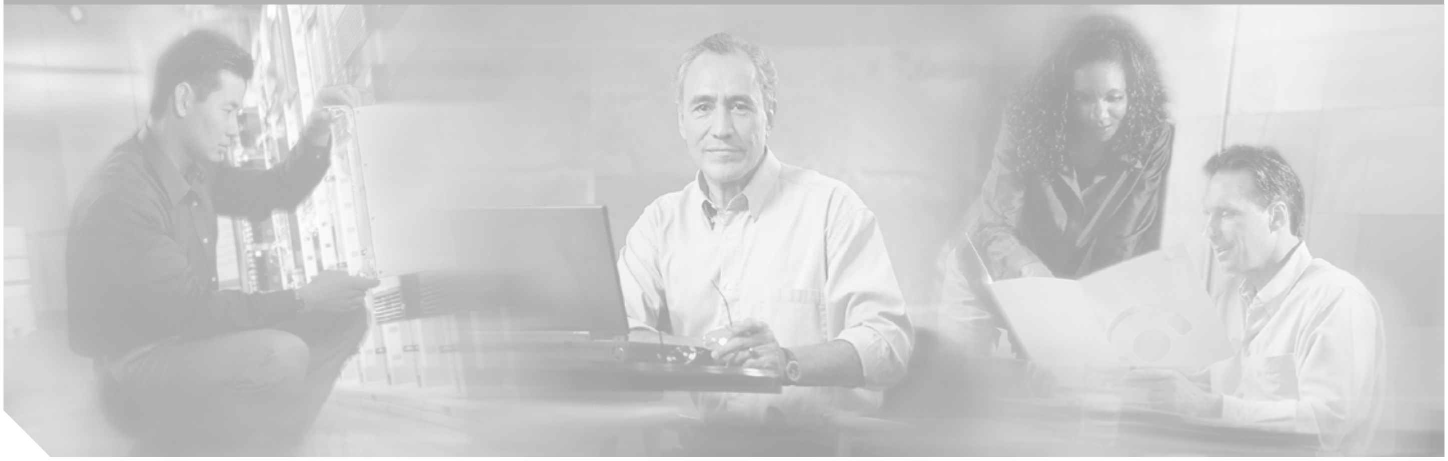
Technical Assistance

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 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.

- **aps clear sonet**
- **aps force sonet**
- **aps lockout sonet**
- **aps manual sonet**
- **aps protect (SONET)**
- **aps unidirectional**
- **show controllers sonet**



Part 3: Virtual Interfaces

Configuring Virtual Interfaces

Virtual interfaces are software-based interfaces that you create in the memory of the networking device using Cisco IOS commands. Virtual interfaces do not have a hardware component such as the RJ-45 female port on a 100BASE-T Fast Ethernet network interface card. This module describes the four common types of virtual, or logical, interfaces that can be configured using Cisco IOS software:

- Loopback interfaces
- Null interfaces
- Subinterfaces
- Tunnel interfaces

Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the "Feature Information for Configuring Virtual Interfaces" section on page 692.

Contents

Prerequisites for Configuring Virtual Interfaces

Before virtual interfaces can be used in your network, you must have some physical (hardware) interfaces configured and be able to communicate between the networking devices on which you wish to use virtual interfaces.

Information About Configuring Virtual Interfaces

To configure virtual interfaces, you should understand the following concepts:

Virtual Interfaces

Virtual interfaces are network interfaces that are not associated with a physical interface. Physical interfaces have some form of physical element—for example, an RJ-45 male connector on an Ethernet cable. Virtual interfaces exist only in software; there are no physical elements. You identify an individual virtual interface using a numerical ID after the virtual interface name. For example: loopback 0, tunnel 1, and fastethernet 0/0.1. The ID is unique per virtual interface type to make the entire name string unique; for example both a loopback 0 interface and a null 0 interface can exist, but two loopback 0 interfaces cannot exist in a single networking device.

Cisco IOS software supports four types of virtual interfaces;

- loopback
- null
- subinterface
- tunnel.

Benefits of Virtual Interfaces

- A loopback interface can provide a stable interface on which you can assign a Layer 3 address such as an IP or IPX address. This address can be configured as the source address when the networking device needs to send data for protocols such as NetFlow or Cisco Discovery Protocol (CDP) to another device in your network and you want the receiving device to always see the same source IP address from the networking device. This is an issue in networks with multiple equal-cost paths because under normal circumstances the packets that are generated by a networking device use the IP address from the outbound interface as the source address for the packets and because in a network with two or more equal-cost paths from the networking device to the receiving host each packet might use a different outbound interface.
- A null interface provides an alternative method of filtering without the overhead involved with using access lists. For example, instead of creating an outbound access list that prevents traffic to a destination network from being transmitted out an interface, you can configure a static route for the destination network that points to the null interface.

- Subinterfaces were invented as a method of virtually subdividing a physical interface into two or more interfaces so that the IP routing protocols would see the network connection to each remote networking device as a separate physical interface even though the subinterfaces share a common physical interface. One of the first uses of subinterfaces was to resolve the problem with split horizon on Frame Relay WANs.
- The following are several situations in which tunneling (encapsulating traffic in another protocol) is useful:
  - To enable multiprotocol local networks over a single-protocol backbone.
  - To provide workarounds for networks that use protocols that have limited hop counts; for example, RIP version 1, AppleTalk.
  - To connect discontiguous subnetworks.
  - To allow virtual private networks across WANs.

Loopback Interfaces

You can specify a software-only interface called a loopback interface to emulate a physical interface. Loopback interfaces are supported on all platforms. A loopback interface is a virtual interface on a Cisco router that remains up (active) after you issue the **no shutdown** command until you disable it with the **shutdown** command. Unlike subinterfaces, loopback interfaces are independent of the state of any physical interface.

The loopback interface can be considered stable because once you enable it, it will remain up until you shut it down. This makes loopback interfaces ideal for assigning Layer 3 addresses such as IP addresses when you want a single address as a reference that is independent of the status of any physical interfaces in the networking device. A good example of this is using the IP address of a loopback interface as the IP address for the DNS host address for the networking device. Before loopback interfaces were available, network administrators had to configure a DNS host entry for every interface on a router that had an IP address assigned to it because they could never be certain which interface IP address might be available at any given time for managing the router. In the sample interface configuration and DNS entries for Router A shown below, you can see that there is a DNS entry for each interface.

Router A Interface Configuration Before Loopback

```
Ethernet0 10.10.10.1 255.255.255.0
Ethernet1 10.10.11.1 255.255.255.0
Ethernet2 10.10.12.1 255.255.255.0
Ethernet3 10.10.13.1 255.255.255.0
Ethernet4 10.10.14.1 255.255.255.0
Ethernet5 10.10.15.1 255.255.255.0
```

Router A DNS Entries Before Loopback

```
RouterA    IN  A  10.10.10.1
           IN  A  10.10.11.1
           IN  A  10.10.12.1
           IN  A  10.10.13.1
           IN  A  10.10.14.1
           IN  A  10.10.15.1
```

Interfaces on networking devices can fail, and they can also be taken out of service for maintenance. If any of the interfaces in Router A fails or is taken out of service, another networking device will not be able to access that interface. When you configure a networking device with a loopback interface and assign it an IP address that is advertised throughout the network, the networking device will be reachable by using this IP address as long as the networking device has at least one network interface capable of sending and receiving IP traffic. In the sample interface configuration and DNS entries for Router A after a loopback interface is configured, you can see that there is now only one DNS entry that can be used to reach the router over any of its physical interfaces.

Router A Interface Configuration After Loopback

```
Loopback 172.16.78.1 255.255.255.0
Ethernet0 10.10.10.1 255.255.255.0
Ethernet1 10.10.11.1 255.255.255.0
Ethernet2 10.10.12.1 255.255.255.0
Ethernet3 10.10.13.1 255.255.255.0
Ethernet4 10.10.14.1 255.255.255.0
Ethernet5 10.10.15.1 255.255.255.0
```

Router A DNS Entries After Loopback

```
RouterA   IN  A  172.16.78.1
```

The configured IP address of the loopback interface—172.16.78.1—can be used as the source address for packets generated by the router and forwarded to networking management applications and routing protocols. Unless this loopback interface is explicitly shut down, it is always reachable.

You can use the loopback interface as the termination address for OSPF or BGP sessions. A loopback interface can also be used to establish a Telnet session from the console port of the device to its auxiliary port when all other interfaces are down. In applications where other routers or access servers attempt to reach this loopback interface, you should configure a routing protocol to distribute the subnet assigned to the loopback address.

IP Packets routed to the loopback interface are rerouted back to the router or access server and processed locally. IP packets routed out the loopback interface but not destined to the loopback interface are dropped. Under these two conditions, the loopback interface can behave like a null interface.

Loopback Interfaces Versus Loopback Mode

Loopback interfaces provide a stable source interface to ensure that the IP address assigned to the interface is always reachable as long as the IP routing protocols continue to advertise the subnet assigned to the loopback interface. Loopback mode, however, is used to test and diagnose issues with WAN (serial) links such as bit loss or data corruption. The idea is to configure a loop to return the data packets that were received by the interface back out the same interface to the device that originated the traffic. Loopback mode is used to troubleshoot problems by checking that the data packets are returned in the same condition in which they were sent. Errors in the data packets indicate a problem with the WAN infrastructure. Many types of serial interfaces have their own form of loopback command syntax that is entered under interface or controller configuration mode.

For more details about loopback mode, see the “Configuring Serial Interfaces” chapter.

Null Interfaces

The null interface is a virtual network interface that is similar to the loopback interface. Whereas traffic to the loopback interface is directed to the router itself, traffic sent to the null interface is discarded. This interface is always up and can never forward or receive traffic; encapsulation always fails. The null interface functions similarly to the null devices available on most operating systems.

Null interfaces are used as a low-overhead method of discarding unnecessary network traffic. For example, if you do not want your network users to be able to reach certain IP subnets, you can create static IP routes for the subnets that point to the null interface of a networking device. Using the static IP routes takes less CPU time for the networking device than using IP access lists. The static-route configuration is also easier to configure than IP access lists because it is done in global configuration mode instead of in interface configuration mode.

The null interface may not be configured with an address. Traffic can be sent to this interface only by configuring a static route where the next hop is the null interface—represented by Null 0. One example of configuring the next hop to be the null interface is to create a route to an aggregate network that can then be announced through the BGP, or to ensure that traffic to a particular range of addresses is not propagated through the router, perhaps for security purposes.

The router always has a single null interface. By default, a packet sent to the null interface causes the router to respond by sending an ICMP unreachable message to the source IP address of the packet. You can configure the router either to send these responses or to drop the packets silently.

Subinterfaces

Subinterfaces are associated with physical interfaces. Subinterfaces are enabled when the physical interface with which they are associated is enabled, and subinterfaces are disabled when the physical interface is shut down.

Note Subinterfaces can be enabled and shut down independently of the physical port with which they are associated. However, you cannot enable a subinterface of a physical interface that has been shut down.

Subinterfaces are created by subdividing the physical interface into two or more virtual interfaces on which you can assign unique Layer 3 network addresses such as IP subnets. One of the first uses of subinterfaces was to resolve the problem with split horizon on Frame Relay WANs. Split horizon is a behavior associated with IP routing protocols such as RIP and OSPF in which IP subnets are not advertised back out the same physical interface that they were learned over. Split horizon was implemented to prevent routing loops in IP networks. A routing loop can be created when the networking devices at both ends of a network connection advertise the same IP routes to each other. Split horizon was an issue for Frame Relay multipoint network interfaces—interfaces that connect to two or more remote networking devices over a single physical interface—because the default behavior of many networking devices was to implement split horizon, which means that the networking device did not advertise the IP routes that were learned over an interface back out the interface to other devices that were also reachable via the same physical interface. Subinterfaces were invented as a method of virtually subdividing a physical interface into two or more interfaces so that the IP routing protocols would see the network connection to each remote networking device as a separate physical interface even though the subinterfaces share a common physical interface. Although TCP/IP now disables split horizon limitations by default, protocols such as AppleTalk and IPX are still constrained by split horizon.

Subinterfaces are identified by a prefix that consists of the hardware interface descriptor (IDB) followed by a period and then by a number that is unique for that prefix. The full subinterface number must be unique to the networking device. For example, the first subinterface for Ethernet interface 0/0 might be named Ethernet 0/0.1 where .1 indicates the subinterface.

Tunnel Interfaces

Tunneling provides a way to encapsulate arbitrary packets inside a transport protocol. Tunnels are implemented as a virtual interface to provide a simple interface for configuration. The tunnel interface is not tied to specific "passenger" or "transport" protocols, but, rather, it is an architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

There are several ways to implement tunnel interfaces depending on the connectivity that you need to provide. One common use for tunnels is to carry data traffic for a network protocol such as IPX over devices in your network that do not support IPX. For instance, if your network uses IPX in sites at the edge of your network but not in the core of your network, you can connect the IPX sites at the network edges by tunneling IPX in IP over the core of the network.

For more details about the various types of tunneling techniques available using Cisco IOS software, see the "Implementing Tunnels" module.

How to Configure Virtual Interfaces

This section contains the following tasks:

- Configuring a Loopback Interface, page 686
- Configuring a Null Interface, page 688

Configuring a Loopback Interface

This task explains how to configure a loopback interface. A loopback interface can be considered stable because once you enable it, it will remain up until you shut it down. This makes loopback interfaces ideal for assigning Layer 3 addresses such as IP addresses to when you want to have a single address to use as a reference that is independent of the status of any of the physical interfaces in the networking device.

Prerequisites

The IP address for the loopback interface must be unique and not in use by another interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *number*
4. **ip address** *ip-address mask* [**secondary**]
5. **end**
6. **show interfaces loopback** *number*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface loopback** *number* **Example:** `Router(config)# interface loopback 0`	Specifies a loopback interface and enters interface configuration mode. • Use the *number* argument to specify the number of the loopback interface that you want to create or configure. **Note** There is no limit on the number of loopback interfaces that you can create.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.20.1.2 255.255.255.0`	Specifies an IP address for the loopback interface and enables IP processing on the interface. • Use the *ip-address* and *mask* arguments to specify the subnet for the loopback address.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 6	**show interfaces loopback** *number* **Example:** `Router# show interfaces loopback 0`	(Optional) Displays information about loopback interfaces. • Use the *number* argument to display information about one particular loopback interface. **Note** Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4.
Step 7	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Examples

The following is sample output for the **show interfaces loopback** command.

```
Router# show interfaces loopback

Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 10.20.1.2/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  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: fifo
  Output queue: 0/0 (size/max)
  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, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuring a Null Interface

This task explains how to configure a null interface. Null interfaces provide an alternative method to access control lists for filtering traffic. All unwanted traffic can be directed to the null interface; the null interface cannot receive or forward traffic, or allow its traffic to be encapsulated.

The only interface configuration command that you can specify for the null interface is the **no ip unreachables** command.

ICMP Unreachable Messages from Null Interfaces

By default, a packet sent to the null interface causes the router to respond by sending an Internet Control Message Protocol (ICMP) unreachable message to the source IP address of the packet. You can configure the router either to send these responses or to drop the packets silently.

To disable the sending of ICMP unreachable messages in response to packets sent to the null interface, use the **no ip unreachables** command in interface configuration mode. To reenable the sending of ICMP unreachable messages in response to packets sent to the null interface, use the **ip unreachables** command in interface configuration mode.

Restrictions

Only one null interface can be configured on each networking device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface null** *number*

4. **no ip unreachables**
5. **end**
6. **show interfaces null** [*number*] [**accounting**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface null** *number* **Example:** `Router(config)# interface null 0`	Specifies a null interface and number, and enters interface configuration mode. - The number argument is always 0.
Step 4	**no ip unreachables** **Example:** `Router(config-if)# no ip unreachables`	Prevents the generation of ICMP unreachable messages on an interface. - This command affects all types of ICMP unreachable messages.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 6	**show interfaces null** [*number*] [**accounting**] **Example:** `Router# show interfaces null 0`	(Optional) Displays information about null interfaces. - For null interfaces, the *number* argument is always 0. **Note** Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4.

Examples

The following is sample output for the **show interfaces null** command.

```
Router# show interfaces null

Null0 is up, line protocol is up
  Hardware is Unknown
  MTU 1500 bytes, BW 10000000 Kbit, DLY 0 usec,
     reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA, loopback not set
  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
  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, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuration Examples for Virtual Interfaces

This section contains the following examples:

- Configuring a Loopback Interface: Example, page 690
- Configuring a Null Interface: Example, page 690

Configuring a Loopback Interface: Example

The following example shows how to configure a loopback interface, loopback 0.

```
interface loopback 0
 ip address 10.20.1.2 255.255.255.0
 end
```

Configuring a Null Interface: Example

The following example shows how to configure a null interface and to drop the ICMP unreachable messages. All packets sent to the null interface are dropped and in this example, the ICMP messages usually sent in response to packets being sent to the null interface are dropped.

```
interface null 0
 no ip unreachables
 end
```

Where to Go Next

- If you want to implement tunnels in your network, see the "Implementing Tunnels" module.
- If you want to implement other types of interfaces such as LAN or serial in your network, see the "Configuring LAN Interfaces" or the "Configuring Serial Interfaces" chapters.

Additional References

The following sections provide references related to virtual interfaces.

Related Documents

Related Topic	Document Title
Interface commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS Interface and Hardware Component Command Reference,* Release 12.4
Configuration example showing how to use loopback interfaces with BGP	*Sample Configuration for iBGP and eBGP With or Without a Loopback Address*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been 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

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of 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/techsupport

Feature Information for Configuring Virtual Interfaces

Table 39 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

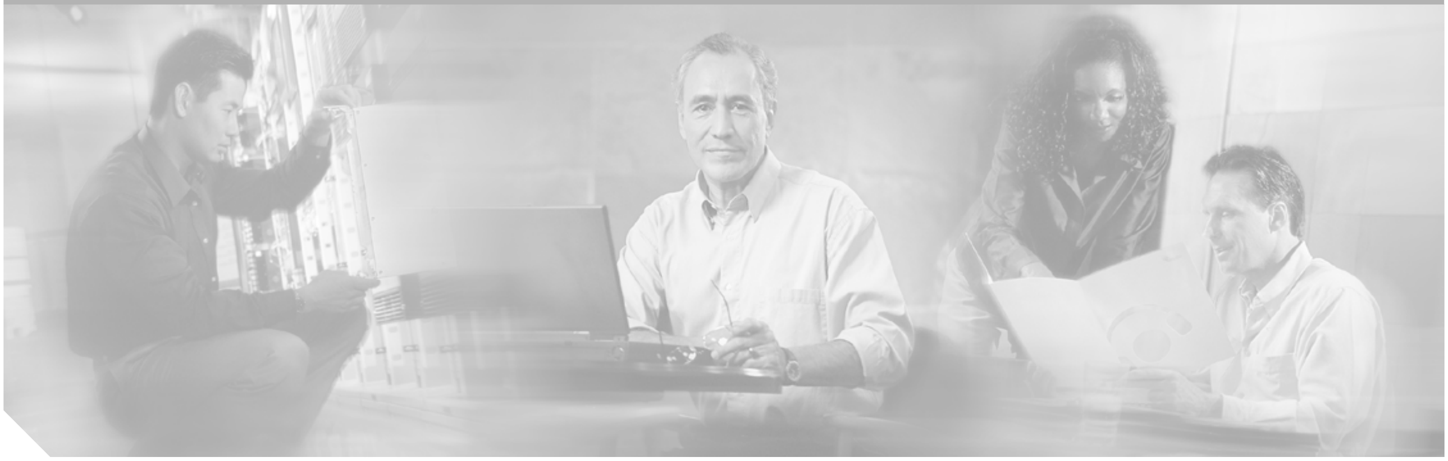
If you are looking for information on a feature in this technology that is not documented here, see the "<<x-ref to the title of the information product roadmap—Section format>>."

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. 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.

Note Table 39 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 39 Feature Information for Configuring Virtual Interfaces

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(1) or later. This table will be updated when feature information is added to this module.	—	—



Part 4: Tunnels

Implementing Tunnels

This module describes the various types of tunneling techniques available using Cisco IOS software. Configuration details and examples are provided for the tunnel types that use physical or virtual interfaces. Many tunneling techniques are implemented using technology-specific commands, and links are provided to the appropriate technology modules.

Tunneling provides a way to encapsulate arbitrary packets inside a transport protocol. Tunnels are implemented as a virtual interface to provide a simple interface for configuration. The tunnel interface is not tied to specific “passenger” or “transport” protocols, but, rather, it is an architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the “Feature Information for Implementing Tunnels” section on page 754.

Contents

Prerequisites for Implementing Tunnels

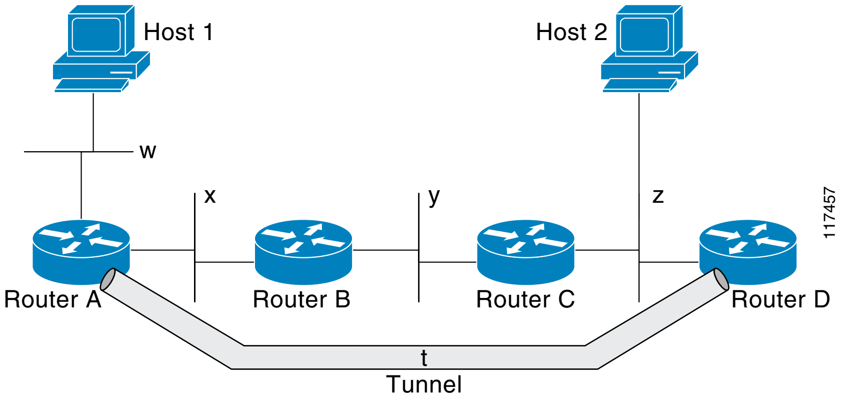
This module assumes that you are running Cisco IOS Release 12.2 or higher.

Restrictions for Implementing Tunnels

- In early versions of Cisco IOS software, only processor switching was supported. Fast switching of generic routing encapsulation (GRE) tunnels was introduced in Cisco IOS Release 11.1. Cisco Express Forwarding (CEF) switching is also now commonly used by the IPv6 and other tunneling protocols.
- It is important to allow the tunnel protocol through a firewall and to allow it to pass access control list (ACL) checking.
- Multiple point-to-point tunnels can saturate the physical link with routing information if the bandwidth is not configured correctly on the tunnel interface.
- A tunnel looks like one hop, and routing protocols may prefer a tunnel over a multihop physical path. This can be deceptive because the tunnel, although it may look like a single hop, may traverse a slower path than a multihop link. A tunnel is as robust and fast, or as unreliable and slow, as the links that it actually traverses. Routing protocols that make their decisions on the sole basis of hop count will often prefer a tunnel over a set of physical links. A tunnel might appear to be a one-hop, point-to-point link and have the lowest-cost path, but may actually cost more in terms of latency than an alternative physical topology.

  For example, in the topology shown in Figure 65, packets from Host 1 will appear to travel across networks w, t, and z to get to Host 2 instead of taking the path w, x, y, and z because the tunnel hop count appears shorter. In fact, the packets going through the tunnel will still be traveling across Router A, B, and C, but they must also travel to Router D before coming back to Router C.

Figure 65 Tunnel Precautions: Hop Counts



- If routing is not carefully configured, the tunnel may have a recursive routing problem. When the best path to the “tunnel destination” is via the tunnel itself, recursive routing causes the tunnel interface to flap. To avoid recursive routing problems, keep the control-plane routing separate from the tunnel routing using the following methods:
  - Use a different autonomous system number or tag.
  - Use a different routing protocol.
  - Use static routes to override the first hop (but watch for routing loops).

  When you have recursive routing to the tunnel destination, the following error appears:

```
%TUN-RECURDOWN Interface Tunnel 0
temporarily disabled due to recursive routing
```

Information About Implementing Tunnels

To configure tunnels, you should understand the following concepts:

Tunneling Versus Encapsulation

To understand how tunnels work, it is important to distinguish between the concepts of encapsulation and tunneling. Encapsulation is the process of adding headers to data at each layer of a particular protocol stack. The Open Systems Interconnection (OSI) reference model describes the functions of a network as seven layers stacked on top of each other. When data has to be sent from one host (a PC for example) on a network to another host, the process of encapsulation is used to add a header in front of the data at each layer of the protocol stack in descending order. The header must contain a data field that indicates the type of data encapsulated at the layer immediately above the current layer. As the packet ascends the protocol stack on the receiving side of the network, each encapsulation header is removed in the reverse order.

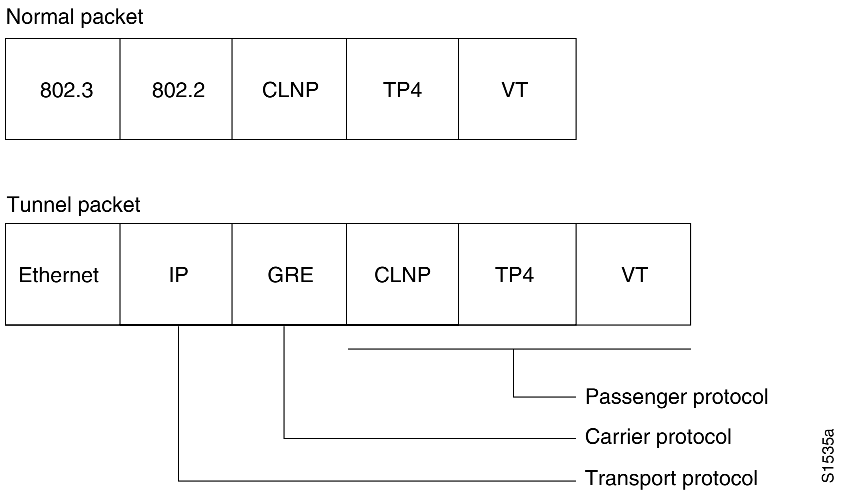
Tunneling encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. Unlike encapsulation, tunneling allows a lower-layer protocol, or same-layer protocol, to be carried through the tunnel. A tunnel interface is a virtual (or logical) interface. For more details on other types of virtual interfaces, see the “Configuring Virtual Interfaces” module. Although many different types of tunnels have been created to solve different network problems, tunneling consists of three main components:

- Passenger protocol—The protocol that you are encapsulating. Examples of passenger protocols are AppleTalk, CLNS, IP, and IPX.
- Carrier protocol—The protocol that does the encapsulating. Examples of carrier protocols are GRE, IP-in-IP, L2TP, MPLS, STUN, and DLSw+.

- Transport protocol—The protocol used to carry the encapsulated protocol. The main transport protocol is IP.

Figure 66 illustrates IP tunneling terminology and concepts.

Figure 66 IP Tunneling Terminology and Concepts



To understand the process of tunneling, consider connecting two AppleTalk networks with a non-AppleTalk backbone, such as IP. The relatively high bandwidth consumed by the broadcasting of Routing Table Maintenance Protocol (RTMP) data packets can severely hamper the backbone's network performance. This problem can be solved by tunneling AppleTalk through a foreign protocol, such as IP. Tunneling encapsulates an AppleTalk packet inside the foreign protocol packet (AppleTalk inside GRE inside IP), which is then sent across the backbone to a destination router. The destination router then removes the encapsulation from the AppleTalk packet and routes the packet.

Definition of Tunneling Types by OSI Layer

Tunnels are used by many different technologies to solve different network challenges, and the resulting variety of tunnel types makes it difficult to determine which tunneling technique to use. The different carrier protocols can be grouped according to the OSI layer model. Table 40 shows the different carrier protocols grouped by OSI layer. Below the table, each carrier protocol is defined, and if the tunnel configuration is not covered within this module, a link to the appropriate module is included.

Table 40 Carrier Protocol by OSI Layer

Layer	Carrier Protocol
2	• PPPoA—Point-to-Point Protocol (PPP) over ATM • PPPoE—PPP over Ethernet • UDLR—Unidirectional link routing
3	• BSTUN—Block Serial Tunneling • CLNS—Connectionless Network Service (CLNS) • GRE—Generic routing encapsulation • IP-in-IP—Internet Protocol encapsulated within IP • IPSec—IP Security • IPv6—IP version 6 • L2F—Layer 2 Forwarding • L2TP—Layer 2 Tunneling Protocol • MPLS—Multiprotocol Label Switching • PPTP—Point-to-Point Tunneling Protocol • STUN—Serial Tunneling
4	• DLSw+—Data-link switching plus • RBSCP—Rate-Based Satellite Control Protocol • SSL—Secure Socket Layer

BSTUN

A Block Serial Tunnel (BSTUN) enables support for devices using the Bisync data-link protocol. This protocol enables enterprises to transport Bisync traffic over the same network that supports their Systems Network Architecture (SNA) and multiprotocol traffic, eliminating the need for separate Bisync facilities.

For more details about configuring BSTUN, see the "Configuring Serial Tunnel and Block Serial Tunnel" chapter in Part 2 of the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.4.

CLNS

The ISO Connectionless Network Service (CLNS) protocol is a standard for the network layer of the OSI model. IP traffic can be transported over CLNS; for instance, on the data communications channel (DCC) of a SONET ring. An IP over CLNS tunnel (CTunnel) is a virtual interface that enhances interactions with CLNS networks, allowing IP packets to be tunneled through the Connectionless Network Protocol (CLNP) to preserve TCP/IP services. CLNS can also be used as a transport protocol with GRE as a carrier protocol (GRE/CLNS), carrying both IPv4 and IPv6 packets.

DLSw+

Data-link switching plus (DLSw+) is Cisco's implementation of the DLSw standard for Systems Network Architecture (SNA) and NetBIOS devices, and it supports several additional features and enhancements. DLSw+ is a means of transporting SNA and NetBIOS traffic over a campus or WAN. The end systems can attach to the network over Token Ring, Ethernet, Synchronous Data Link Control

(SDLC), Qualified Logical Link Control (QLLC), or Fiber Distributed Data Interface (FDDI). DLSw+ switches between diverse media and locally terminates the data links, keeping acknowledgments, keepalives, and polling off the WAN.

For more details about configuring DLSw+, see the "Configuring Data-Link Switching Plus" chapter in Part 2 of the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.4.

GRE

Generic routing encapsulation (GRE) is defined in RFC 2784. GRE is a carrier protocol that can be used with a variety of underlying transport protocols, and GRE can carry a variety of passenger protocols. RFC 2784 also covers the use of GRE with IPv4 as the transport protocol and the passenger protocol. Cisco IOS software supports GRE as the carrier protocol with many combinations of passenger and transport protocols.

For more details about GRE, see the "Generic Routing Encapsulation" section on page 704.

IP-in-IP

IP-in-IP is a Layer 3 tunneling protocol—defined in RFC 2003—that alters the normal routing of an IP packet by encapsulating it within another IP header. The encapsulating header specifies the address of a router that would not ordinarily be selected as a next-hop router on the basis of the real destination address of the packet. The intermediate node decapsulates the packet, which is then routed to the destination as usual.

IPSec

In simple terms, IP Security (IPSec) provides secure tunnels between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these packets by specifying characteristics of these tunnels. IPSec peers set up a secure tunnel and encrypt the packets that traverse the tunnel to the remote peer.

IPSec also works with the GRE and IP-in-IP, L2F, L2TP, and DLSw+ tunneling protocols; however, multipoint tunnels are not supported. Other Layer 3 tunneling protocols may not be supported for use with IPSec.

For more details about configuring IPSec, see the "Configuring Security for VPNs with IPSec" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4.

IPv6

IP version 6 (IPv6) is a new version of the Internet Protocol based on and designed as the successor to IP version 4. IPv6 adds a much larger address space—128 bits—and improvements such as a simplified main header and extension headers. IPv6 is described initially in RFC 2460, *Internet Protocol, Version 6 (IPv6)*. The use of IPv6 as a carrier protocol is described in RFC 2473, *Generic Packet Tunneling in IPv6 Specification*.

L2F

Layer 2 Forwarding (L2F) tunneling is used in virtual private dialup networks (VPDNs). A VPDN allows separate and autonomous protocol domains to share common access infrastructure including modems, access servers, and ISDN routers by the tunneling of link-level (Layer 2) frames. Typical L2F tunneling use includes Internet service providers (ISPs) or other access service creating virtual tunnels to link to remote customer sites or remote users with corporate intranet or extranet networks.

For more details about configuring L2F, see the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.

L2TP

Layer 2 Tunneling Protocol (L2TP) is an open standard created by the Internet Engineering Task Force (IETF) that uses the best features of L2F and Point-to-Point Tunneling Protocol (PPTP). L2TP is designed to secure the transmission of IP packets across uncontrolled and untrusted network domains, and it is an important component of Virtual Private Networks (VPNs). VPNs extend remote access to users over a shared infrastructure while maintaining the same security and management policies as a private network.

For more details about configuring L2TP, see the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.

MPLS

Multiprotocol Label Switching (MPLS) is a high-performance packet forwarding technology that integrates the performance and traffic management capabilities of data-link-layer (Layer 2) switching with the scalability, flexibility, and performance of network-layer (Layer 3) routing. The MPLS architecture has been designed to allow data to be transferred over any combination of Layer 2 technologies, to support all Layer 3 protocols, and to scale. Using Cisco Express Forwarding (CEF), MPLS can efficiently enable the delivery of IP services over an ATM switched network. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering.

For more details about how MPLS traffic engineering uses tunnels, see the "MPLS Traffic Engineering" module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide,* Release 12.4.

PPPoA

PPP over ATM (PPPoA) is mainly implemented as part of Asymmetric Digital Subscriber Line (ADSL). It relies on RFC 1483, operating in either Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) or VC-Mux mode. A customer premises equipment (CPE) device encapsulates the PPP session based on this RFC for transport across the ADSL loop and the digital subscriber line access multiplexer (DSLAM).

For more details about configuring PPPoA, see the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.

PPPoE

RFC 2516 defines PPP over Ethernet (PPPoE) as providing the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator or aggregation concentrator. As customers deploy ADSL, they must support PPP-style authentication and authorization over a large installed base of legacy bridging customer premises equipment (CPE). Using a form of tunneling encapsulation, PPPoE allows each host to use its own PPP stack, thus presenting the user with a familiar user interface. Access control, billing, and type of service (ToS) can be done on a per-user, rather than a per-site, basis.

For more details about configuring PPPoE, see the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client enterprise server by creating a VPN across TCP/IP data networks. PPTP supports on-demand, multiprotocol, virtual private networking over public networks such as the Internet.

For more details about configuring PPTP, see the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.

RBSCP

Rate-Based Satellite Control Protocol (RBSCP) was designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IP Security (IPSec), over satellite links without breaking the end-to-end model.

SSL Tunnels

Secure Socket Layer (SSL) is designed to make use of TCP sessions to provide a reliable end-to-end secure service. The main role of SSL is to provide security for web traffic. Security includes confidentiality, message integrity, and authentication. SSL achieves these elements of security through the use of cryptography, digital signatures, and certificates. SSL protects confidential information through the use of cryptography. Sensitive data is encrypted across public networks to achieve a level of confidentiality.

SSL is implemented using the Cisco Application and Content Networking System (ACNS). For more details about configuring SSL, see the latest *Cisco ACNS Software Deployment and Configuration Guide*.

STUN

Cisco's Serial Tunneling (STUN) implementation allows Synchronous Data Link Control (SDLC) protocol devices and High-Level Data Link Control (HDLC) devices to connect to one another through a multiprotocol internetwork rather than through a direct serial link. STUN encapsulates SDLC frames in either the TCP/IP or the HDLC protocol. STUN provides a straight passthrough of all SDLC traffic (including control frames, such as Receiver Ready) end-to-end between Systems Network Architecture (SNA) devices.

For more details about configuring STUN, see the "Configuring Serial Tunnel and Block Serial Tunnel" chapter in Part 2 of the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.4.

UDLR Tunnels

Unidirectional link routing (UDLR) provides mechanisms for a router to emulate a bidirectional link to enable the routing of unicast and multicast packets over a physical unidirectional interface, such as a broadcast satellite link. However, there must be a back channel or other path between the routers that share a physical unidirectional link (UDL). A UDLR tunnel is a mechanism for unicast and multicast traffic; Internet Group Management Protocol (IGMP) UDLR is a related technology for multicast traffic.

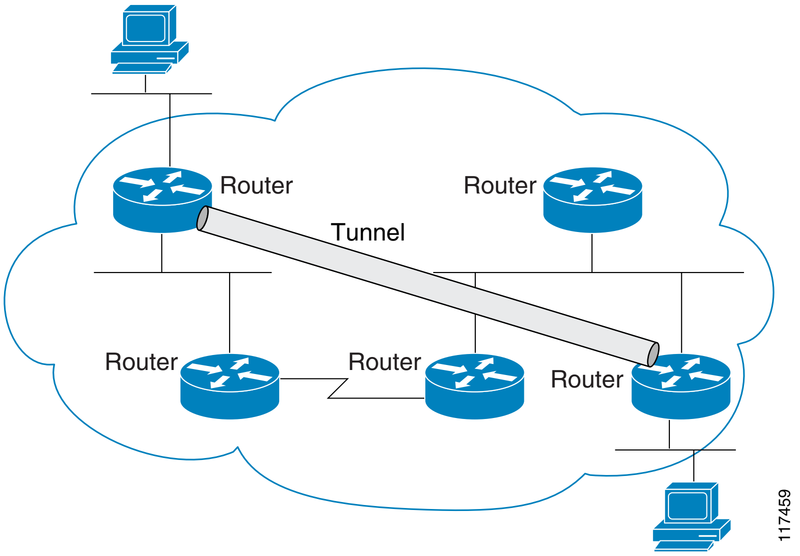
For more details about UDLR tunneling, see *Cisco IOS IP Multicast Configuration Guide*, Release 12.4.

Benefits of Tunneling

The following are several situations in which tunneling (encapsulating traffic in another protocol) is useful:

- To enable multiprotocol local networks over a single-protocol backbone.
- To provide workarounds for networks that use protocols that have limited hop counts; for example, RIP version 1, AppleTalk (see Figure 67).
- To connect discontiguous subnetworks.
- To allow virtual private networks across WANs.

Figure 67 Providing Workarounds for Networks with Limited Hop Counts



If the path between two computers has more than 15 hops, the computers cannot communicate with each other, but it is possible to hide some of the hops inside the network using a tunnel.

Tunnel ToS

Tunnel type of service (ToS) allows you to tunnel your network traffic and group all your packets in the same specific ToS byte value. The ToS byte values and Time-to-Live (TTL) hop-count value can be set in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. The Tunnel ToS feature is supported for Cisco Express Forwarding (CEF), fast switching, and process switching.

The ToS and TTL byte values are defined in RFC 791. RFC 2474 and RFC 2780 obsolete the use of the ToS byte as defined in RFC 791. RFC 791 specifies that bits 6 and 7 of the ToS byte (the first two least significant bits) are reserved for future use and should be set to 0. Currently, the Tunnel ToS feature does not conform to this standard and allows you to set the whole ToS byte value, including bits 6 and 7, and decide to which RFC standard the ToS byte of your packets should confirm.

Mobile IP Tunneling

New devices and business practices, such as PDAs and the next-generation of data-ready cellular phones and services, are driving interest in the ability of a user to roam while maintaining network connectivity. The requirement for data connectivity solutions for this group of users is very different than it is for the fixed dialup user or the stationary wired LAN user. Solutions need to accommodate the challenge of movement during a data session or conversation.

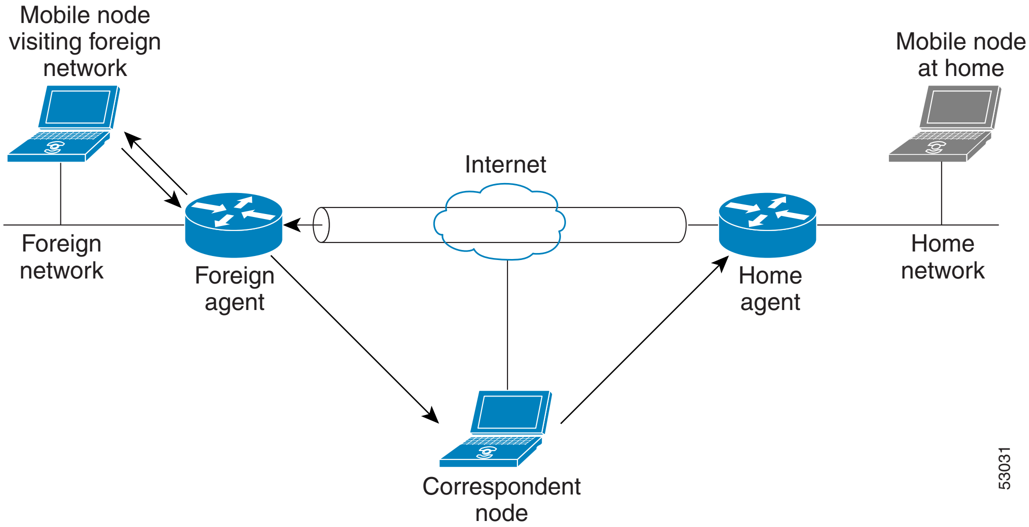
Mobile IP is a tunneling-based solution that takes advantage of the Cisco-created generic routing encapsulation (GRE) tunneling technology and simpler IP-in-IP tunneling protocol.

Mobile IP is comprised of the following three components, as shown in Figure 68:

- Mobile node (MN)
- Home agent (HA)

- Foreign agent (FA)

Figure 68 Mobile IP Components and Use of Tunneling



An MN is a node, for example, a PDA, a laptop computer, or a data-ready cellular phone, that can change its point of attachment from one network or subnet to another. This node can maintain ongoing communications while using only its home IP address. In Figure 68, the current location of the MN—a laptop computer—is shown in bold.

An HA is a router on the home network of the MN that maintains an association between the home IP address of the MN and its *care-of address*, which is the current location of the MN on a foreign or visited network. The HA redirects packets by tunneling them to the MN while it is away from home.

An FA is a router on a foreign network that assists the MN in informing its HA of its current care-of address. The FA detunnels packets that were tunneled by the HA and delivers them to the MN. The FA also acts as the default router for packets generated by the MN while it is connected to the foreign network.

The traffic destined for the MN is forwarded in a triangular manner. When a device on the Internet, called a correspondent node (CN), sends a packet to the MN, the packet is routed to the home network of the MN, the HA redirects the packet by tunneling to the care-of address (current location) of the MN on the foreign network, as shown in Figure 68. The FA receives the packet from the HA and forwards it locally to the MN. However, packets sent by the MN are routed directly to the CN.

For more details about configuring Mobile IP, see the *Cisco IOS IP Mobility Configuration Guide*, Release 12.4.

Generic Routing Encapsulation

Generic routing encapsulation (GRE) is defined in RFC 2784. GRE is a carrier protocol that can be used with a variety of underlying transport protocols and that can carry a variety of passenger protocols. RFC 2784 also covers the use of GRE with IPv4 as the transport protocol and the passenger protocol. Cisco IOS software supports GRE as the carrier protocol with many combinations of passenger and transport protocols such as:

- GRE over an IPv4 network (GRE/IPv4)—GRE is the carrier protocol, and IPv4 is the transport protocol. This is the most common type of GRE tunnel. For configuration details, see the "Configuring a GRE Tunnel" section on page 716. Cisco IOS software supports many passenger protocols for GRE/IPv4 such as AppleTalk, IPX, IPv4, and IPv6. For more details about IPv6 as a passenger protocol with GRE/IPv4, see the "GRE/IPv4 Tunnel Support for IPv6 Traffic" section on page 705.
- GRE over a CLNS network (GRE/CLNS)—GRE is the carrier protocol, and CLNS is the transport protocol. This is described in RFC 3147. For more details about CLNS as a passenger protocol with GRE/CLNS, see the "GRE/CLNS Tunnel Support for IPv4 and IPv6 Packets" section on page 705.
- GRE over an IPv6 network (GRE/IPv6)—GRE is the carrier protocol, and IPv6 is the transport protocol. Cisco IOS software supports IPv4 and IPv6 as passenger protocols with GRE/IPv6. For configuration details about IPv4 and IPv6 as passenger protocols with GRE/IPv6, see the "Configuring GRE/IPv6 Tunnels" section on page 719.

Multipoint GRE Tunneling

Enhanced multipoint GRE (mGRE) tunneling technology provides a Layer 3 (L3) transport mechanism for use in IP networks. This same dynamic Layer 3 tunneling transport can be used within IP networks to transport VPN traffic across service provider and enterprise networks, as well as to provide interoperability for packet transport between IP and MPLS VPNs. This feature provides support for RFC 2547, which defines the outsourcing of IP-backbone services for enterprise networks.

Multipoint tunnels use the Next Hop Resolution Protocol (NHRP) in the same way that a Frame Relay multipoint interface uses information obtained by the reverse ARP mechanism to learn the Layer 3 addresses of the remote data-link connection identifiers (DLCIs).

In Cisco IOS Release 12.2(8)T and later releases, CEF-switching over mGRE tunnels was introduced. Previously, only process switching was available for mGRE tunnels. CEF-switching over mGRE tunnels enables CEF switching of IP traffic to and from multipoint GRE tunnels. Tunnel traffic can be forwarded to a prefix through a tunnel destination when both the prefix and the tunnel destination are specified by the application.

GRE/CLNS Tunnel Support for IPv4 and IPv6 Packets

GRE tunneling of IPv4 and IPv6 packets through CLNS networks enables Cisco CLNS tunnels (CTunnels) to interoperate with networking equipment from other vendors. This feature provides compliance with RFC 3147.

The optional GRE services defined in header fields, such as checksums, keys, and sequencing, are not supported. Any packet that is received and requests such services will be dropped.

GRE/IPv4 Tunnel Support for IPv6 Traffic

IPv6 traffic can be carried over IPv4 generic routing encapsulation (GRE) tunnels using the standard GRE tunneling technique that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. As in IPv6 manually configured tunnels, GRE tunnels are links between two points, with a separate tunnel for each link. The tunnels are not tied to a specific passenger or transport protocol, but in this case IPv6 is the passenger protocol, GRE is the carrier protocol, and IPv4 is the transport protocol.

The primary use of GRE tunnels is for stable connections that require regular secure communication between two edge routers or between an edge router and an end system. The edge routers and the end systems must be dual-stack implementations.

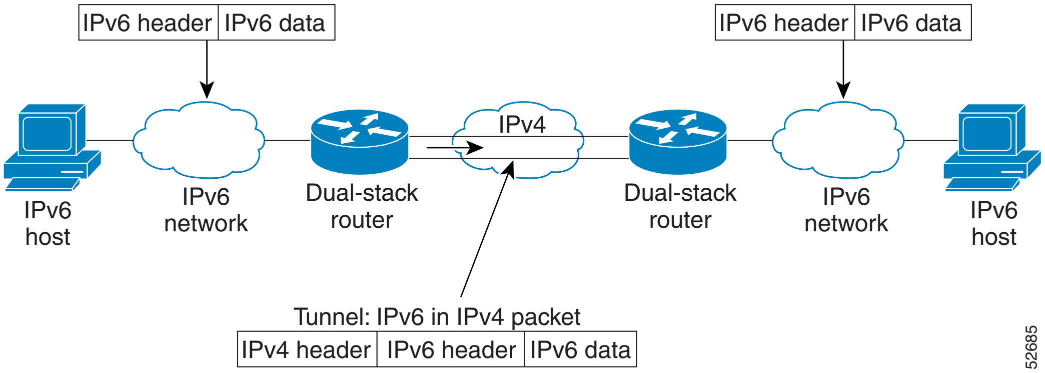
GRE has a protocol field that identifies the passenger protocol. GRE tunnels allow IS-IS or IPv6 to be specified as a passenger protocol, allowing both IS-IS and IPv6 traffic to run over the same tunnel. If GRE did not have a protocol field, it would be impossible to distinguish whether the tunnel was carrying IS-IS or IPv6 packets. The GRE protocol field is why it is desirable that you tunnel IS-IS and IPv6 inside GRE.

Overlay Tunnels for IPv6

Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure (a core network or the Internet). (See Figure 69.) By using overlay tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Overlay tunnels can be configured between border routers or between a border router and a host; however, both tunnel endpoints must support both the IPv4 and IPv6 protocol stacks. Cisco IOS IPv6 currently supports the following types of overlay tunneling mechanisms:

- Manual
- Generic routing encapsulation (GRE)
- IPv4-compatible
- 6to4
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

Figure 69 Overlay Tunnels



Note Overlay tunnels reduce the maximum transmission unit (MTU) of an interface by 20 octets (assuming that the basic IPv4 packet header does not contain optional fields). A network that uses overlay tunnels is difficult to troubleshoot. Therefore, overlay tunnels that connect isolated IPv6 networks should not be considered as a final IPv6 network architecture. The use of overlay tunnels should be considered as a transition technique toward a network that supports both the IPv4 and IPv6 protocol stacks or just the IPv6 protocol stack.

Use Table 41 to help you determine which type of tunnel you want to configure to carry IPv6 packets over an IPv4 network.

Table 41 Suggested Usage of Tunnel Types to Carry IPv6 Packets over an IPv4 Network

Tunneling Type	Suggested Usage	Usage Notes
Manual	Simple point-to-point tunnels that can be used within a site or between sites.	Can carry IPv6 packets only.
GRE/IPv4	Simple point-to-point tunnels that can be used within a site or between sites.	Can carry IPv6, CLNS, and many other types of packets.
Compatible	Point-to-multipoint tunnels.	Uses the ::/96 prefix. We do not now recommend using this tunnel type.
6to4	Point-to-multipoint tunnels that can be used to connect isolated IPv6 sites.	Sites use addresses from the 2002::/16 prefix.
ISATAP	Point-to-multipoint tunnels that can be used to connect systems within a site.	Sites can use any IPv6 unicast addresses.

Individual tunnel types are discussed in more detail in the following concepts, and we recommend that you review and understand the information on the specific tunnel type that you want to implement. When you are familiar with the type of tunnel you need, Table 42 provides a quick summary of the tunnel configuration parameters that you may find useful.

Table 42 Overlay Tunnel Configuration Parameters by Tunneling Type

Overlay Tunneling Type	Overlay Tunnel Configuration Parameter			
	Tunnel Mode	Tunnel Source	Tunnel Destination	Interface Prefix/Address
Manual	**ipv6ip**	An IPv4 address or a reference to an interface on which IPv4 is configured.	An IPv4 address.	An IPv6 address.
GRE/IPv4	**gre ip**		An IPv4 address.	An IPv6 address.
Compatible	**ipv6ip auto-tunnel**		Not required. These are all point-to-multipoint tunneling types. The IPv4 destination address is calculated, on a per-packet basis, from the IPv6 destination.	Not required. The interface address is generated as ::*tunnel-source*/96
6to4	**ipv6ip 6to4**			An IPv6 address. The prefix must embed the tunnel source IPv4 address
ISATAP	**ipv6ip isatap**			An IPv6 prefix in modified eui-64 format. The IPv6 address is generated from the prefix and the tunnel source IPv4 address.

IPv6 Manually Configured Tunnels

A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone. The primary use is for stable connections that require regular secure communication between two edge routers or between an end system and an edge router, or for connection to remote IPv6 networks.

An IPv6 address is manually configured on a tunnel interface, and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks. Manually configured tunnels can be configured between border routers or between a border router and a host. Cisco Express Forwarding (CEF) switching can be used for IPv6 manually configured tunnels, or CEF switching can be disabled if process switching is needed.

Automatic 6to4 Tunnels

An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. The key difference between automatic 6to4 tunnels and manually configured tunnels is that the tunnel is not point-to-point; it is point-to-multipoint. In automatic 6to4 tunnels, routers are not configured in pairs because they treat the IPv4 infrastructure as a virtual nonbroadcast multiaccess (NBMA) link. The IPv4 address embedded in the IPv6 address is used to find the other end of the automatic tunnel.

An automatic 6to4 tunnel may be configured on a border router in an isolated IPv6 network, which creates a tunnel on a per-packet basis to a border router in another IPv6 network over an IPv4 infrastructure. The tunnel destination is determined by the IPv4 address of the border router extracted from the IPv6 address that starts with the prefix 2002::/16, where the format is 2002:*border-router-IPv4-address*::/48. Following the embedded IPv4 address are 16 bits that can be used to number networks within the site. The border router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks. 6to4 tunnels are configured between border routers or between a border router and a host.

The simplest deployment scenario for 6to4 tunnels is to interconnect multiple IPv6 sites, each of which has at least one connection to a shared IPv4 network. This IPv4 network could be the global Internet or a corporate backbone. The key requirement is that each site have a globally unique IPv4 address; the Cisco IOS software uses this address to construct a globally unique 6to4/48 IPv6 prefix. As with other tunnel mechanisms, appropriate entries in a Domain Name System (DNS) that map between hostnames and IP addresses for both IPv4 and IPv6 allow the applications to choose the required address.

Automatic IPv4-Compatible IPv6 Tunnels

Automatic IPv4-compatible tunnels use IPv4-compatible IPv6 addresses. IPv4-compatible IPv6 addresses are IPv6 unicast addresses that have zeros in the high-order 96 bits of the address and an IPv4 address in the low-order 32 bits. They can be written as 0:0:0:0:0:0:A.B.C.D or ::A.B.C.D, where “A.B.C.D” represents the embedded IPv4 address.

The tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses. The host or router at each end of an IPv4-compatible tunnel must support both the IPv4 and IPv6 protocol stacks. IPv4-compatible tunnels can be configured between border routers or between a border router and a host. Using IPv4-compatible tunnels is an easy method to create tunnels for IPv6 over IPv4, but the technique does not scale for large networks.

Note IPv4-compatible tunnels were initially supported for IPv6, but are currently being deprecated. Cisco now recommends that you use a different IPv6 tunneling technique named ISATAP tunnels.

ISATAP Tunnels

The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an automatic overlay tunneling mechanism that uses the underlying IPv4 network as a nonbroadcast multiaccess (NBMA) link layer for IPv6. ISATAP is designed for transporting IPv6 packets *within* a site where a native IPv6 infrastructure is not yet available; for example, when sparse IPv6 hosts are deployed for testing. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to communicate with other such hosts on the same virtual link, basically creating an IPv6 network using the IPv4 infrastructure.

The ISATAP router provides standard router advertisement network configuration support for the ISATAP site. This feature allows clients to automatically configure themselves as they would do if they were connected to an Ethernet. It can also be configured to provide connectivity out of the site. ISATAP uses a well-defined IPv6 address format composed of any unicast IPv6 prefix (/64), which can be link-local or global (including 6to4 prefixes), enabling IPv6 routing locally or on the Internet. The IPv4 address is encoded in the last 32 bits of the IPv6 address, enabling automatic IPv6-in-IPv4 tunneling.

While the ISATAP tunneling mechanism is similar to other automatic tunneling mechanisms, such as IPv6 6to4 tunneling, ISATAP is designed for transporting IPv6 packets *within* a site, not *between* sites.

ISATAP uses unicast addresses that include a 64-bit IPv6 prefix and a 64-bit interface identifier. The interface identifier is created in modified EUI-64 format in which the first 32 bits contain the value 000:5EFE to indicate that the address is an IPv6 ISATAP address. Table 43 shows the layout of an ISATAP address.

Table 43 IPv6 ISATAP Address Format

64 Bits	32 Bits	32 Bits
Link local or global IPv6 unicast prefix	0000:5EFE	IPv4 address of the ISATAP link

As shown in Table 43, an ISATAP address consists of an IPv6 prefix and the ISATAP interface identifier. This interface identifier includes the IPv4 address of the underlying IPv4 link. The following example shows what an actual ISATAP address would look like if the prefix is 2001:0DB8:1234:5678::/64 and the embedded IPv4 address is 10.173.129.8. In the ISATAP address, the IPv4 address is expressed in hexadecimal as 0AAD:8108.

Example

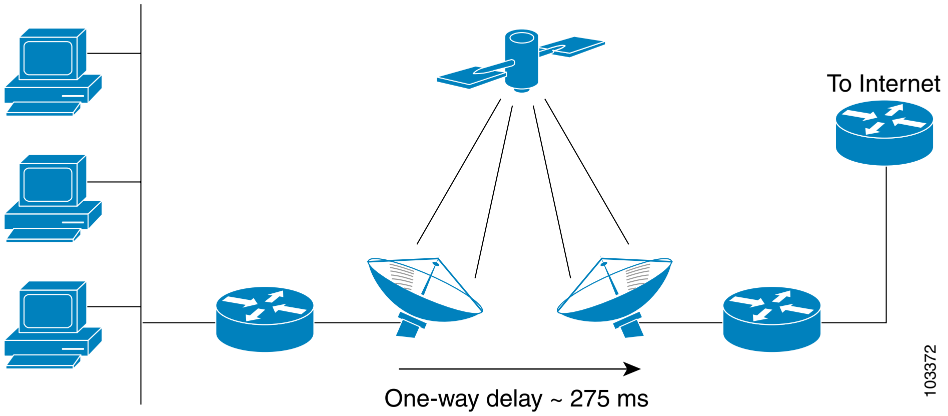
2001:0DB8:1234:5678:0000:5EFE:0AAD:8108

Rate-Based Satellite Control Protocol Tunnels

Rate-Based Satellite Control Protocol (RBSCP) was designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IP Security (IPSec), over satellite links without breaking the end-to-end model.

Satellite links have several characteristics that affect the performance of IP protocols over the link. Figure 70 shows that satellite links can have a one-way delay of 275 milliseconds. A round-trip time (RTT) of 550 milliseconds is a very long delay for TCP. Another issue is the high error rates (packet loss rates) that are typical of satellite links as compared to wired links in LANs. Even the weather affects satellite links, causing a decrease in available bandwidth and an increase in RTT and packet loss.

Figure 70 Typical Satellite Link

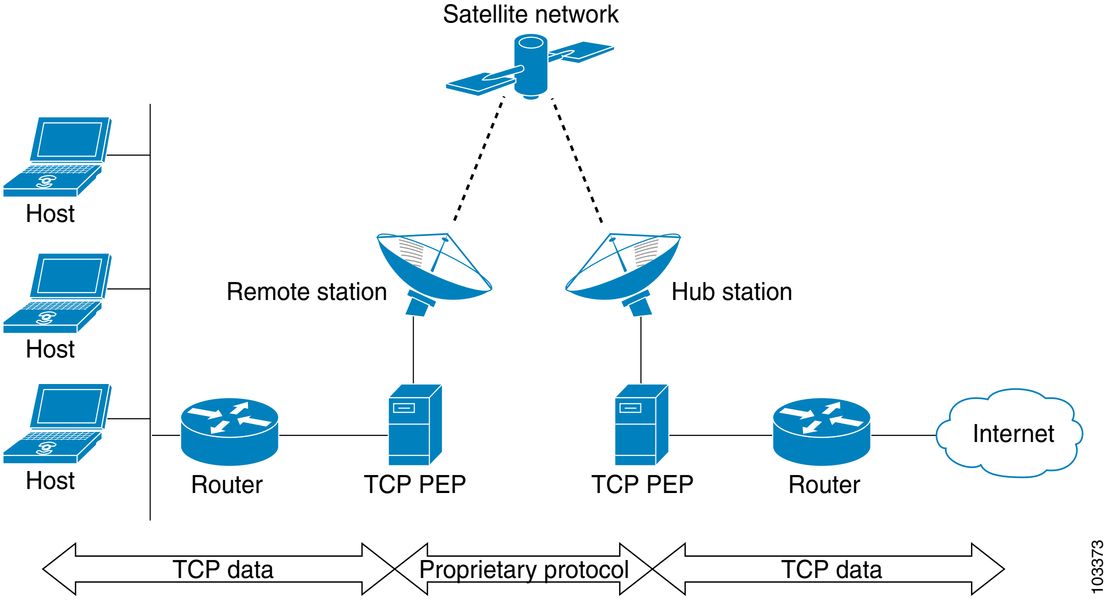


Long RTT keeps TCP in a slow start mode, which increases the time before the satellite link bandwidth is fully used. TCP and Stream Control Transmission Protocol (SCTP) interpret packet loss events as congestion in the network and start to perform congestion recovery procedures, which reduce the traffic being sent over the link.

Although available satellite link bandwidths are increasing, the long RTT and high error rates experienced by IP protocols over satellite links are producing a high bandwidth-delay product (BDP).

To address the problem of TCP being kept in a slow start mode when a satellite link is used, a disruptive performance enhancing proxy (PEP) solution is often introduced into the network. In Figure 71 you can see that the transport connection is broken up into three sections with hosts on the remote side connecting to the Internet through their default router. The router sends all Internet-bound traffic to the TCP PEP, which terminates the TCP connection to the Internet. The PEP generates a local TCP ACK (TCP spoofing) for all data. Traffic is buffered and retransmitted through a single PEP protocol connection over the satellite link. The second PEP receives the data from the satellite link and retransmits the data over separate TCP connections to the Internet. TCP transmission is disrupted, so dropped packets are not interpreted as TCP congestion and can be retransmitted from buffered data. Minimal TCP ACKs and reduced TCP slow starts allow more bandwidth to be used.

Figure 71 Disruptive TCP PEP Solution

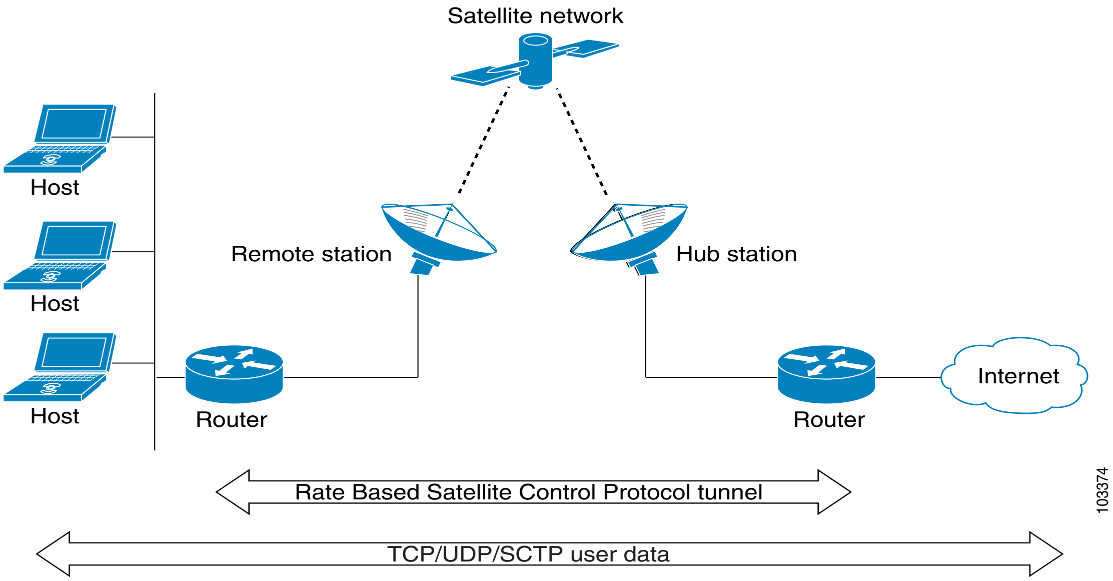


One of the disadvantages to using disruptive TCP PEP is the breaking of the end-to-end model. Some applications cannot work when the flow of traffic is broken, and the PEP has no provision for handling encrypted traffic (IPSec). New transport protocols such as SCTP require special handling or additional code to function with disruptive TCP PEP. An additional managed network component is also required at every satellite router.

RBSCP has been designed to preserve the end-to-end model and provide performance improvements over the satellite link without using a PEP solution. IPSec encryption of clear-text traffic (for example a VPN service configuration) across the satellite link is supported. RBSCP allows two routers to control and monitor the sending rates of the satellite link, thereby increasing the bandwidth utilization. Lost packets are retransmitted over the satellite link by RBSCP, preventing the end host TCP senders from going into slow start mode.

RBSCP is implemented using a tunnel interface as shown in Figure 72. The tunnel can be configured over any network interface supported by Cisco IOS software that can be used by a satellite modem or internal satellite modem network module. IP traffic is sent across the satellite link with appropriate modifications and enhancements that are determined by the router configuration. Standard routing or policy-based routing can be used to determine the traffic to be sent through the RBSCP tunnel.

Figure 72 Nondisruptive RBSCP Solution



RBSCP tunnels can be configured for any of the following features:

- **Time Delay**—One of the RBSCP routers can be configured to hold frames due for transmission through the RBSCP tunnel. The delay time increases the RTT at the end host and allows RBSCP time to retransmit lost TCP frames or other protocol frames. If the retransmission is successful, it prevents lost frame events from reaching the end host where congestion procedures would be enabled. In some cases the retransmission can be completed by RBSCP without inserting the delay. This option should be used only when the RTT of the satellite link is greater than 700 milliseconds.
- **ACK Splitting**—Performance improvements can be made for clear-text TCP traffic using acknowledgement (ACK) splitting in which a number of additional TCP ACKs are generated for each TCP ACK received. TCP will open a congestion window by one maximum transmission unit (MTU) for each TCP ACK received. Opening the congestion window results in increased bandwidth becoming available. Configure this feature only when the satellite link is not using all the available bandwidth. Encrypted traffic cannot use ACK splitting.
- **Window Stuffing**—Clear-text TCP and SCTP traffic can benefit from the RBSCP window stuffing feature. RBSCP can buffer traffic so that the advertised window can be incremented up to the available satellite link bandwidth or the available memory in the router. The end host that sends the packets is fooled into thinking that a larger window exists at the receiving end host and sends more traffic. Use this feature with caution because the end host may send too much traffic for the satellite link to handle and the resulting loss and retransmission of packets may cause link congestion.
- **SCTP Drop Reporting**—SCTP uses an appropriate byte counting method instead of ACK counting to determine the size of the transmission window, so ACK splitting does not work with SCTP. The RBSCP tunnel can generate an SCTP packet-dropped report for packets dropped across the satellite but not as a result of congestion loss. This SCTP drop reporting is on by default and provides a chance to retransmit the packet without affecting the congestion window size. Actual congestion losses are still reported, and normal recovery mechanisms are activated.

Path MTU Discovery

Path MTU Discovery (PMTUD) can be enabled on a GRE or IP-in-IP tunnel interface. When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the GRE (or IP-in-IP) tunnel IP packets. The router always performs PMTUD processing on the original data IP packets that enter the tunnel. When PMTUD is enabled, packet fragmentation is not permitted for packets that traverse the tunnel because the Don't Fragment (DF) bit is set on all the packets. If a packet that enters the tunnel encounters a link with a smaller MTU, the packet is dropped and an ICMP message is sent back to the sender of the packet. This message indicates that fragmentation was required (but not permitted) and provides the MTU of the link that caused the packet to be dropped.

For more detailed information about PMTUD, see the *IP Fragmentation and PMTUD* document.

Note PMTUD on a tunnel interface requires that the tunnel endpoint be able to receive ICMP messages generated by routers in the path of the tunnel. Check that ICMP messages can be received before using PMTUD over firewall connections.

Use the **tunnel path-mtu-discovery** command to enable PMTUD for the tunnel packets, and use the **show interfaces tunnel** command to verify the tunnel PMTUD parameters. PMTUD currently works only on GRE and IP-in-IP tunnel interfaces.

QoS Options for Tunnels

A tunnel interface supports many of the same quality of service (QoS) features as a physical interface. QoS provides a way to ensure that mission-critical traffic has an acceptable level of performance. QoS options for tunnels include support for applying generic traffic shaping (GTS) directly on the tunnel interface and support for class-based shaping using the modular QoS command-line interface (MQC). Tunnel interfaces also support class-based policing, but they do not support committed access rate (CAR).

Note Service policies are not supported on tunnel interfaces on Cisco 7500 series routers.

GRE tunnels allow the router to copy the IP precedence bit values of the type of service (ToS) byte to the tunnel or the GRE IP header that encapsulates the inner packet. Intermediate routers between the tunnel endpoints can use the IP precedence values to classify the packets for QoS features such as policy routing, weighted fair queueing (WFQ), and weighted random early detection (WRED).

When packets are encapsulated by tunnel or encryption headers, QoS features are unable to examine the original packet headers and correctly classify the packets. Packets that travel across the same tunnel have the same tunnel headers, so the packets are treated identically if the physical interface is congested. Tunnel packets can, however, be classified before tunneling and encryption can occur by using the QoS preclassify feature on the tunnel interface or on the crypto map.

Note Class-based WFQ (CBWFQ) inside class-based shaping is not supported on a multipoint interface.

For examples of how to implement some QoS features on a tunnel interface, see the "Configuring QoS Options on Tunnel Interfaces: Examples" section on page 750.

How to Implement Tunnels

This section contains the following tasks:

- Determining the Tunnel Type, page 714 (required)
- Configuring a GRE Tunnel, page 716 (optional)
- Configuring GRE/IPv6 Tunnels, page 719 (optional)
- Configuring a CTunnel, page 721 (optional)
- Configuring GRE/CLNS CTunnels to Carry IPv4 and IPv6 Packets, page 722 (optional)
- Configuring Manual IPv6 Tunnels, page 725 (optional)
- Configuring 6to4 Tunnels, page 726 (optional)
- Configuring IPv4-Compatible IPv6 Tunnels, page 728 (optional)
- Configuring ISATAP Tunnels, page 729 (optional)
- Configuring the RBSCP Tunnel, page 731 (optional)
- Verifying Tunnel Configuration and Operation, page 733 (optional)
- Verifying RBSCP Tunnel Configuration and Operation, page 735 (optional)

Determining the Tunnel Type

Before configuring a tunnel, you must determine what type of tunnel you need to create.

SUMMARY STEPS

1. Determine the passenger protocol.
2. Determine the tunnel CLI type.
3. Determine the **tunnel mode** command keyword, if appropriate.

DETAILED STEPS

Step 1 Determine the passenger protocol.

The passenger protocol is the protocol that you are encapsulating.

Step 2 Determine the tunnel CLI type.

Table 44 shows how to determine the tunnel command-line interface (CLI) command required for the transport protocol that you are using in the tunnel.

Table 44 Determining the Tunnel CLI by the Transport Protocol

Transport Protocol	Tunnel CLI Command
CLNS	**ctunnel** (with optional **mode gre** keywords)
Other	**tunnel mode** (with appropriate keyword)

Step 3 Determine the **tunnel mode** command keyword, if appropriate.

Table 45 shows how to determine the appropriate keyword to use with the **tunnel mode** command. In the tasks that follow in this module, only the relevant keywords for the **tunnel mode** command are displayed.

Table 45 Determining the tunnel mode Command Keyword

Keyword	Purpose
dvmrp	Use the **dvmrp** keyword to specify that the Distance Vector Multicast Routing Protocol encapsulation will be used.
gre ip	Use the **gre ip** keywords to specify that GRE encapsulation over IP will be used.
gre ipv6	Use the **gre ipv6** keywords to specify that GRE encapsulation over IPv6 will be used.
gre multipoint	Use the **gre multipoint** keywords to specify that multipoint GRE (mGRE) encapsulation will be used.
ipip [**decapsulate-any**]	Use the **ipip** keyword to specify that IP-in-IP encapsulation will be used. The optional **decapsulate-any** keyword terminates any number of IP-in-IP tunnels at one tunnel interface. Note that this tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipv6	Use the **ipv6** keyword to specify that generic packet tunneling in IPv6 will be used.
ipv6ip	Use the **ipv6ip** keyword to specify that IPv6 will be used as the passenger protocol and IPv4 as both the carrier (encapsulation) and transport protocol. When additional keywords are not used, manual IPv6 tunnels are configured. Additional keywords can be used to specify IPv4-compatible, 6to4, or ISATAP tunnels.
mpls	Use the **mpls** keyword to specify that MPLS will be used for configuring Traffic Engineering (TE) tunnels.
rbscp	Use the **rbscp** keyword to specify that RBSCP tunnels will be used.

What to Do Next

- To configure a tunnel to carry IP data packets, proceed to the "Configuring a GRE Tunnel" section on page 716.
- To configure a tunnel to carry CLNS data packets, proceed to the "Configuring a CTunnel" section on page 721.
- To configure a tunnel to carry IPv4 and IPv6 data packets over a CLNS network, proceed to the "Configuring GRE/CLNS CTunnels to Carry IPv4 and IPv6 Packets" section on page 722.

- To configure a tunnel to carry IPv6 data packets, review the "Overlay Tunnels for IPv6" section on page 706 and proceed to one of the following tasks:
  - "Configuring GRE/IPv6 Tunnels" section on page 719
  - "Configuring Manual IPv6 Tunnels" section on page 725
  - "Configuring 6to4 Tunnels" section on page 726
  - "Configuring IPv4-Compatible IPv6 Tunnels" section on page 728
  - "Configuring ISATAP Tunnels" section on page 729
- To configure an RBSCP tunnel to carry IP data packets over a satellite or other long-distance delay link with high error rates, proceed to the "Configuring the RBSCP Tunnel" section on page 731.

Configuring a GRE Tunnel

Perform this task to configure a GRE tunnel. A tunnel interface is used to pass protocol traffic across a network that does not normally support the protocol. To build a tunnel, a tunnel interface must be defined on each of two routers and the tunnel interfaces must reference each other. At each router, the tunnel interface must be configured with a Layer 3 address. The tunnel endpoints, tunnel source, and tunnel destination must be defined, and the type of tunnel must be selected. Optional steps can be performed to customize the tunnel.

Remember to configure the router at each end of the tunnel. If only one side of a tunnel is configured, the tunnel interface may still come up and stay up (unless keepalive is configured), but packets going into the tunnel will be dropped.

In Cisco IOS Release 12.2(8)T and later releases, CEF-switching over multipoint GRE tunnels was introduced. Previously, only process switching was available for multipoint GRE tunnels.

GRE Tunnel Keepalive

Keepalive packets can be configured to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side.

Prerequisites

Ensure that the physical interface to be used as the tunnel source in this task is up and configured with the appropriate IP address. For hardware technical descriptions and information about installing interfaces, see the hardware installation and configuration publication for your product.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bandwidth** *kbps*
5. **keepalive** [*period* [*retries*]]
6. **tunnel source** {*ip-address* | *interface-type interface-number*}

7. **tunnel destination** {*hostname* | *ip-address*}
8. **tunnel key** *key-number*
9. **tunnel mode** {**gre ip** | **gre multipoint**}
10. **ip mtu** *bytes*
11. **ip tcp mss** *mss-value*
12. **tunnel path-mtu-discovery** [**age-timer** {*aging-mins* | **infinite**}]
13. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface`** *`type number`*
	Example:
	`Router(config)# interface tunnel 0`
		Specifies the interface type and number and enters interface configuration mode.
		• To configure a tunnel, use **tunnel** for the *type* argument.
		• On some router platforms such as the Cisco 7500 series, the number argument may consist of a slot, port adapter, and port number. For more details, see the **interface** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4.

Step 4	**`bandwidth`** *`kbps`*
	Example:
	`Router(config-if)# bandwidth 1000`
		Sets the current bandwidth value for an interface and communicates it to higher-level protocols. Specifies the tunnel bandwidth to be used to transmit packets.
		• Use the *kbps* argument to set the bandwidth, in kilobits per second (kbps).
		Note This is a routing parameter only; it does not affect the physical interface. The default bandwidth setting on a tunnel interface is 9.6 kbps. You should set the bandwidth on a tunnel to an appropriate value.

	Command or Action	Purpose

Step 5	`keepalive [period [retries]]`
	Example:
	`Router(config-if)# keepalive 3 7`
		(Optional) Specifies the number of times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down.
		- GRE keepalive packets may be sent from both sides of a tunnel or from just one side. If they are sent from both sides, the *period* and *retries* arguments can be different at each side of the link. If you configure keepalives on only one side of the tunnel, only one side will detect a problem and shut down. The other side will continue to route packets into the tunnel, and these packets will be dropped.
		Note This command is supported only on GRE point-to-point tunnels.

Step 6	`tunnel source {ip-address | interface-type interface-number}`
	Example:
	`Router(config-if)# tunnel source Ethernet 1`
		Configures the tunnel source.
		- Use the *ip-address* argument to specify the source IP address.
		- Use the *interface-type* and *interface-number* arguments to specify the interface to use.

Step 7	`tunnel destination {hostname | ip-address}`
	Example:
	`Router(config-if)# tunnel destination 172.17.2.1`
		Configures the tunnel destination.
		- Use the *hostname* argument to specify the name of the host destination.
		- Use the *ip-address* argument to specify the IP address of the host destination.

Step 8	`tunnel key key-number`
	Example:
	`Router(config-if)# tunnel key 1000`
		(Optional) Enables an ID key for a tunnel interface.
		- Use the *key-number* argument to identify a tunnel key that is carried in each packet.
		- Tunnel ID keys can be used as a form of weak security to prevent improper configuration or injection of packets from a foreign source.
		Note This command is supported only on GRE tunnel interfaces. We do not recommend relying on this key for security purposes.

Step 9	`tunnel mode {gre ip | gre multipoint}`
	Example:
	`Router(config-if)# tunnel mode gre ip`
		Specifies the encapsulation protocol to be used in the tunnel.
		- Use the **gre ip** keywords to specify that GRE over IP encapsulation will be used.
		- Use the **gre multipoint** keywords to specify that multipoint GRE (mGRE) will be used.

	Command or Action	Purpose
Step 10	**ip mtu** *bytes* **Example:** `Router(config-if)# ip mtu 1400`	(Optional) Set the maximum transmission unit (MTU) size of IP packets sent on an interface. • If an IP packet exceeds the MTU set for the interface, the Cisco IOS software will fragment it unless the DF bit is set. • All devices on a physical medium must have the same protocol MTU in order to operate. **Note** If the **tunnel path-mtu-discovery** command is enabled in Step 12, do not configure this command.
Step 11	**ip tcp mss** *mss-value* **Example:** `Router(config-if)# ip tcp mss 250`	(Optional) Specifies the maximum segment size (MSS) for TCP connections that originate or terminate on a router. • Use the *mss-value* argument to specify the maximum segment size for TCP connections, in bytes.
Step 12	**tunnel path-mtu-discovery** [**age-timer** {*aging-mins* | **infinite**}] **Example:** `Router(config-if)# tunnel path-mtu-discovery`	(Optional) Enables Path MTU Discovery (PMTUD) on a GRE or IP-in-IP tunnel interface. • When PMTUD is enabled on a tunnel interface, PMTUD will operate for GRE IP tunnel packets to minimize fragmentation in the path between the tunnel endpoints.

Step 13	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring GRE/IPv6 Tunnels

This task explains how to configure a GRE tunnel on an IPv6 network. GRE tunnels can be configured to run over an IPv6 network layer and to transport IPv6 packets in IPv6 tunnels and IPv4 packets in IPv6 tunnels.

Prerequisites

When GRE/IPv6 tunnels are configured, IPv6 addresses are assigned to the tunnel source and the tunnel destination. The tunnel interface can have either IPv4 or IPv6 addresses assigned (this is not shown in the task below). The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface tunnel** *tunnel-number*
4. **tunnel source** {*ipv6-address* | *interface-type interface-number*}
5. **tunnel destination** *ipv6-address*
6. **tunnel mode gre ipv6**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *tunnel-number* **Example:** `Router(config)# interface tunnel 0`	Specifies a tunnel interface and number, and enters interface configuration mode.

Step 4	**tunnel source** {*ipv6-address* | *interface-type interface-number*}
	Example:
	`Router(config-if)# tunnel source ethernet 0`
		Specifies the source IPv6 address or the source interface type and number for the tunnel interface.
		• If an interface type and number are specified, that interface must be configured with an IPv6 address.
		Note Only the syntax used in this context is displayed. For more details, see the *Cisco IOS IPv6 Command Reference*.

Step 5	**tunnel destination** *ipv6-address* **Example:** `Router(config-if)# tunnel destination 2001:0DB8:0C18:2::300`	Specifies the destination IPv6 address for the tunnel interface. **Note** Only the syntax used in this context is displayed. For more details, see the *Cisco IOS IPv6 Command Reference*.
Step 6	**tunnel mode gre ipv6** **Example:** `Router(config-if)# tunnel mode gre ipv6`	Specifies a GRE IPv6 tunnel. **Note** The **tunnel mode gre ipv6** command specifies GRE as the encapsulation protocol for the tunnel.

Step 7	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring a CTunnel

Perform this task to configure an IP over CLNS tunnel (CTunnel). To configure a CTunnel between a single pair of routers, a tunnel interface must be configured with an IP address, and a tunnel destination must be defined. The destination network service access point (NSAP) address for Router A would be the NSAP address of Router B, and the destination NSAP address for Router B would be the NSAP address of Router A. Ideally, the IP addresses used for the virtual interfaces at either end of the tunnel should be in the same IP subnet. Remember to configure the router at each end of the tunnel.

CTunnel

A CTunnel lets you transport IP traffic over Connectionless Network Service (CLNS); for example, on the data communications channel (DCC) of a SONET ring. CTunnels allow IP packets to be tunneled through the Connectionless Network Protocol (CLNP) to preserve TCP/IP services.

Configuring a CTunnel allows you to telnet to a remote router that has only CLNS connectivity. Other management facilities can also be used, such as Simple Network Management Protocol (SNMP) and TFTP, which otherwise would not be available over a CLNS network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ctunnel** *interface-number*
4. **ip address** *ip-address mask*
5. **ctunnel destination** *remote-nsap-address*
6. **end**
7. **show interfaces ctunnel** *interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface ctunnel** *interface-number* **Example:** `Router(config)# interface ctunnel 102`	Creates a virtual interface to transport IP over a CLNS tunnel and enters interface configuration mode. **Note** The interface number must be unique for each CTunnel interface.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	Enables IP on the interface. • Use the *ip-address* and *mask* arguments to specify the IP address and mask for the interface.
Step 5	**ctunnel destination** *remote-nsap-address* **Example:** `Router(config-if)# ctunnel destination 49.0001.2222.2222.2222.00`	Specifies the destination NSAP address of the CTunnel, where the packets exit the tunnel. • Use the *remote-nsap-address* argument to specify the NSAP address at the CTunnel endpoint.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 7	**show interfaces ctunnel** *interface-number* **Example:** `Router# show interfaces ctunnel 102`	(Optional) Displays information about an IP over CLNS tunnel. • Use the *interface-number* argument to specify a CTunnel interface. • Use this command to verify the CTunnel configuration.

Troubleshooting Tips

Use the **ping** command to diagnose basic network connectivity issues.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring GRE/CLNS CTunnels to Carry IPv4 and IPv6 Packets

Perform this task to configure a CTunnel in GRE mode to transport IPv4 and IPv6 packets in a CLNS network.

To configure a CTunnel between a single pair of routers, a tunnel interface must be configured with an IP address, and a tunnel destination must be defined. The destination network service access point (NSAP) address for Router A would be the NSAP address of Router B, and the destination NSAP address for Router B would be the NSAP address of Router A. Ideally, the IP addresses used for the virtual interfaces at either end of the tunnel should be in the same IP subnet. Remember to configure the router at each end of the tunnel.

Tunnels for IPv4 and IPv6 Packets over CLNS Networks

Configuring the **ctunnel mode gre** command on a CTunnel interface enables IPv4 and IPv6 packets to be tunneled over CLNS in accordance with RFC 3147. Compliance with this RFC should allow interoperation between Cisco equipment and that of other vendors in which the same standard is implemented.

RFC 3147 specifies the use of GRE for tunneling packets. The implementation of this feature does not include support for GRE services defined in header fields, such as those used to specify checksums, keys, or sequencing. Any packets received that specify the use of these features will be dropped.

The default CTunnel mode continues to use the standard Cisco encapsulation, which will tunnel only IPv4 packets. If you want to tunnel IPv6 packets, you must use the GRE encapsulation mode. Both ends of the tunnel must be configured with the same mode for either method to work.

Prerequisites

- An IPv4 or IPv6 address must be configured on a CTunnel interface, and manually configured CLNS addresses must be assigned to the CTunnel destination.
- The host or router at each end of a configured CTunnel must support both the IPv4 and IPv6 protocol stacks.
- Both CTunnel source and destination must be configured to run in the same mode.

Restrictions

GRE services, such as those used to specify checksums, keys, or sequencing, are not supported. Packets that request use of those features will be dropped.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ctunnel** *interface-number*
4. **ip address** *ip-address mask*

   or

   ipv6 address *ipv6-prefix***/***prefix-length* [**eui-64**]
5. **ctunnel destination** *remote-nsap-address*
6. **ctunnel mode gre**
7. **end**
8. **show interfaces ctunnel** *interface-number*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface ctunnel`** *`interface-number`*
	Example:
	`Router(config)# interface ctunnel 102`
		Creates a virtual interface to transport IP over a CLNS tunnel and enters interface configuration mode.
		Note The interface number must be unique for each CTunnel interface.

Step 4	**`ip address`** *`ip-address mask`*
	or
	`ipv6 address` *`ipv6-prefix`***`/`***`prefix-length`* `[`**`eui-64`**`]`
	Example:
	`Router(config-if)# ipv6 address 2001:0DB8:1234:5678::3/126`
		Specifies the IPv4 or IPv6 network assigned to the interface and enables IPv4 or IPv6 packet processing on the interface.
		Note See the "Implementing Basic Connectivity for IPv6" module for more information on configuring IPv6 addresses.

Step 5	**`ctunnel destination`** *`remote-nsap-address`*
	Example:
	`Router(config-if)# ctunnel destination 192.168.30.1`
		Specifies the destination NSAP address of the CTunnel, where the packets are extracted.
		• Use the *remote-nsap-address* argument to specify the NSAP address at the CTunnel endpoint.

Step 6	**`ctunnel mode gre`**
	Example:
	`Router(config-if)# ctunnel mode gre`
		Specifies a CTunnel running in GRE mode for both IPv4 and IPv6 traffic.
		Note The **ctunnel mode gre** command specifies GRE as the encapsulation protocol for the tunnel.

Step 7	**`end`**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 8	**`show interfaces ctunnel`** *`interface-number`*
	Example:
	`Router# show interfaces ctunnel 102`
		(Optional) Displays information about an IP over CLNS tunnel.
		• Use the *interface-number* argument to specify a CTunnel interface.
		• Use this command to verify the CTunnel configuration.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring Manual IPv6 Tunnels

This task explains how to configure a manual IPv6 overlay tunnel.

Prerequisites

With manually configured IPv6 tunnels, an IPv6 address is configured on a tunnel interface and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix***/***prefix-length* [**eui-64**]
5. **tunnel source** {*ip-address* **|** *interface-type interface-number*}
6. **tunnel destination** *ip-address*
7. **tunnel mode ipv6ip**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface tunnel** *tunnel-number* **Example:** Router(config)# interface tunnel 0	Specifies a tunnel interface and number, and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-prefix***/***prefix-length* [**eui-64**] **Example:** Router(config-if)# ipv6 address 2001:0DB8:1234:5678::3/126	Specifies the IPv6 network assigned to the interface and enables IPv6 processing on the interface. **Note** See the "Configuring Basic Connectivity for IPv6" module for more information on configuring IPv6 addresses.

	Command or Action	Purpose

Step 5	**tunnel source** {*ip-address* | *interface-type interface-number*}
	Example:
	`Router(config-if)# tunnel source ethernet 0`
		Specifies the source IPv4 address or the source interface type and number for the tunnel interface.
		• If an interface is specified, the interface must be configured with an IPv4 address.

Step 6	**tunnel destination** *ip-address* **Example:** `Router(config-if)# tunnel destination 192.168.30.1`	Specifies the destination IPv4 address for the tunnel interface.
Step 7	**tunnel mode ipv6ip** **Example:** `Router(config-if)# tunnel mode ipv6ip`	Specifies a manual IPv6 tunnel. **Note** The **tunnel mode ipv6ip** command specifies IPv6 as the passenger protocol and IPv4 as both the carrier (encapsulation) and transport protocol for the manual IPv6 tunnel.

Step 8	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring 6to4 Tunnels

This task explains how to configure a 6to4 overlay tunnel.

Prerequisites

With 6to4 tunnels, the tunnel destination is determined by the border-router IPv4 address, which is concatenated to the prefix 2002::/16 in the format 2002:*border-router-IPv4-address*::/48. The border router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks.

Restrictions

The configuration of only one IPv4-compatible tunnel and one 6to4 IPv6 tunnel is supported on a router. If you choose to configure both of these tunnel types on the same router, we strongly recommend that they not share the same tunnel source.

The reason that a 6to4 tunnel and an IPv4-compatible tunnel cannot share the same interface is that both of them are NBMA "point-to-multipoint" access links and only the tunnel source can be used to reorder the packets from a multiplexed packet stream into a single packet stream for an incoming interface. So when a packet with an IPv4 protocol type of 41 arrives on an interface, that packet is mapped to an IPv6 tunnel interface on the basis of the IPv4 address. However, if both the 6to4 tunnel and the IPv4-compatible tunnel share the same source interface, the router cannot determine the IPv6 tunnel interface to which it should assign the incoming packet.

IPv6 manually configured tunnels can share the same source interface because a manual tunnel is a "point-to-point" link, and both the IPv4 source and IPv4 destination of the tunnel are defined.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix***/***prefix-length* [**eui-64**]
5. **tunnel source** {*ip-address* | *interface-type interface-number*}
6. **tunnel mode ipv6ip 6to4**
7. **exit**
8. **ipv6 route** *ipv6-prefix***/***prefix-length* **tunnel** *tunnel-number*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface tunnel`** *`tunnel-number`*
	Example:
	`Router(config)# interface tunnel 0`
		Specifies a tunnel interface and number, and enters interface configuration mode.

Step 4	**`ipv6 address`** *`ipv6-prefix`***`/`***`prefix-length`* `[`**`eui-64`**`]`
	Example:
	`Router(config-if)# ipv6 address 2002:c0a8:6301:1::1/64`
		Specifies the IPv6 address assigned to the interface and enables IPv6 processing on the interface.
		• The 32 bits following the initial 2002::/16 prefix correspond to an IPv4 address assigned to the tunnel source.
		Note See the "Configuring Basic Connectivity for IPv6" module for more information on configuring IPv6 addresses.

Step 5	**`tunnel source`** `{`*`ip-address`* `|` *`interface-type interface-number`*`}`
	Example:
	`Router(config-if)# tunnel source ethernet 0`
		Specifies the source IPv4 address or the source interface type and number for the tunnel interface.
		Note The interface type and number specified in the **tunnel source** command must be configured with an IPv4 address.

	Command or Action	Purpose

Step 6	**`tunnel mode ipv6ip 6to4`**
	Example:
	`Router(config-if)# tunnel mode ipv6ip 6to4`
		Specifies an IPv6 overlay tunnel using a 6to4 address.

Step 7	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode and returns to global configuration mode.

Step 8	**`ipv6 route`** *`ipv6-prefix`*/*`prefix-length`* **`tunnel`** *`tunnel-number`*
	Example:
	`Router(config)# ipv6 route 2002::/16 tunnel 0`
		Configures a static route for the IPv6 6to4 prefix 2002::/16 to the specified tunnel interface.
		Note When configuring a 6to4 overlay tunnel, you must configure a static route for the IPv6 6to4 prefix 2002::/16 to the 6to4 tunnel interface.
		• The tunnel number specified in the **ipv6 route** command must be the same tunnel number specified in the **interface tunnel** command.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring IPv4-Compatible IPv6 Tunnels

This task explains how to configure an IPv4-compatible IPv6 overlay tunnel.

Prerequisites

With an IPv4-compatible tunnel, the tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses. The host or router at each end of an IPv4-compatible tunnel must support both the IPv4 and IPv6 protocol stacks.

Restrictions

IPv4-compatible tunnels were initially supported for IPv6, but Cisco now recommends that you use a different IPv6 overlay tunneling technique.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **tunnel source** {*ip-address* | *interface-type interface-number*}
5. **tunnel mode ipv6ip auto-tunnel**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface tunnel`** *`tunnel-number`*
	Example:
	`Router(config)# interface tunnel 0`
		Specifies a tunnel interface and number, and enters interface configuration mode.

Step 4	**`tunnel source`** `{`*`ip-address`* `|` *`interface-type interface-number`*`}`
	Example:
	`Router(config-if)# tunnel source ethernet 0`
		Specifies the source IPv4 address or the source interface type and number for the tunnel interface.
		Note The interface type and number specified in the **tunnel source** command must be configured with an IPv4 address.

Step 5	**`tunnel mode ipv6ip auto-tunnel`**
	Example:
	`Router(config-if)# tunnel mode ipv6ip auto-tunnel`
		Specifies an IPv4-compatible tunnel using an IPv4-compatible IPv6 address.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring ISATAP Tunnels

This task describes how to configure an ISATAP overlay tunnel.

Prerequisites

The **tunnel source** command used in the configuration of an ISATAP tunnel must point to an interface that is configured with an IPv4 address. The ISATAP IPv6 address and prefix (or prefixes) advertised are configured for a native IPv6 interface. The IPv6 tunnel interface must be configured with a modified EUI-64 address because the last 32 bits in the interface identifier are constructed using the IPv4 tunnel source address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix***/***prefix-length* [**eui-64**]
5. **no ipv6 nd suppress-ra**
6. **tunnel source** {*ip-address* | *interface-type interface-number*}
7. **tunnel mode ipv6ip isatap**
8. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface tunnel`** *`tunnel-number`*
	Example:
	`Router(config)# interface tunnel 1`
		Specifies a tunnel interface and number, and enters interface configuration mode.

Step 4	**`ipv6 address`** *`ipv6-prefix`*`/`*`prefix-length`* `[`**`eui-64`**`]`
	Example:
	`Router(config-if)# ipv6 address 2001:0DB8:6301::/64 eui-64`
		Specifies the IPv6 address assigned to the interface and enables IPv6 processing on the interface.
		Note See the "Configuring Basic Connectivity for IPv6" module for more information on configuring IPv6 addresses.

Step 5	**`no ipv6 nd suppress-ra`**
	Example:
	`Router(config-if)# no ipv6 nd suppress-ra`
		Enables the sending of IPv6 router advertisements to allow client autoconfiguration.
		• Sending of IPv6 router advertisements is disabled by default on tunnel interfaces.

Step 6	**`tunnel source`** `{`*`ip-address`* `|` *`interface-type interface-number`*`}`
	Example:
	`Router(config-if)# tunnel source ethernet 1/0/1`
		Specifies the source IPv4 address or the source interface type and number for the tunnel interface.
		Note The interface type and number specified in the **tunnel source** command must be configured with an IPv4 address.

Step 7	**`tunnel mode ipv6ip isatap`**
	Example:
	`Router(config-if)# tunnel mode ipv6ip isatap`
		Specifies an IPv6 overlay tunnel using an ISATAP address.

Step 8	**`end`**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

Proceed to the "Verifying Tunnel Configuration and Operation" section on page 733.

Configuring the RBSCP Tunnel

Perform this task to configure the RBSCP tunnel. Remember to configure the router at each end of the tunnel.

Prerequisites

Ensure that the physical interface to be used as the tunnel source in this task is already configured.

Restrictions

- RBSCP was designed for wireless or long-distance delay links with high error rates such as satellite links. If you do not have long-distance delay links with high error rates, do not implement this feature.
- If IP access control lists (ACLs) are configured on an interface that is used by an RBSCP tunnel, the RBSCP IP protocol (199) must be allowed to enter and exit that interface or the tunnel will not function.
- RBSCP has some performance limitations because traffic through the tunnel is process-switched.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip unnumbered** *interface-type interface-number*
5. **tunnel source** {*ip-address* | *interface-type interface-number*}
6. **tunnel destination** {*hostname* | *ip-address*}
7. **tunnel bandwidth** {**receive** | **transmit**} *bandwidth*
8. **tunnel mode rbscp**
9. **tunnel rbscp ack-split** *split-size*
10. **tunnel rbscp delay**
11. **tunnel rbscp report**
12. **tunnel rbscp window-stuff** *step-size*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface tunnel 0`	Specifies the interface type and number and enters interface configuration mode.
Step 4	**ip unnumbered** *interface-type interface-number* **Example:** `Router(config-if)# ip unnumbered Ethernet 1`	Enables IP processing on an interface without assigning an explicit IP address. - Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet.

Step 5	**tunnel source** {*ip-address* | *interface-type interface-number*}
	Example:
	`Router(config-if)# tunnel source Ethernet 1`
		Configures the tunnel source.
		- Use the *ip-address* argument to specify the IP address of the service provider.
		- Use the *interface-type* and *interface-number* arguments to specify the interface to use. For RBSCP we recommend specifying an interface as the tunnel source.

Step 6	**tunnel destination** {*hostname* | *ip-address*}
	Example:
	`Router(config-if)# tunnel destination 172.17.2.1`
		Configures the tunnel destination.
		- Use the *hostname* argument to specify the name of the host destination.
		- Use the *ip-address* argument to specify the IP address of the host destination.

Step 7	**tunnel bandwidth** {**receive** | **transmit**} *bandwidth* **Example:** `Router(config-if)# tunnel bandwidth transmit 1000`	Specifies the tunnel bandwidth to be used to transmit packets. - Use the *bandwidth* argument to specify the bandwidth. **Note** The **receive** keyword is no longer used.
Step 8	**tunnel mode rbscp** **Example:** `Router(config-if)# tunnel mode rbscp`	Specifies the protocol to be used in the tunnel. - Use the **rbscp** keyword to specify that RBSCP will be used as the tunnel protocol.

	Command or Action	Purpose
Step 9	**tunnel rbscp ack-split** *split-size* **Example:** `Router(config-if)# tunnel rbscp ack-split 6`	(Optional) Enables TCP acknowledgement (ACK) splitting with RBSCP tunnels. • Use the *split-size* argument to specify the number of ACKs to send for every ACK received. • The default number of ACKs is 4.
Step 10	**tunnel rbscp delay** **Example:** `Router(config-if)# tunnel rbscp delay`	(Optional) Enables RBSCP tunnel delay. • Use this command only when the RTT measured between the two routers nearest to the satellite links is greater than 700 milliseconds.
Step 11	**tunnel rbscp report** **Example:** `Router(config-if)# tunnel rbscp report`	(Optional) Reports dropped RBSCP packets to SCTP. • Reporting dropped packets to SCTP provides better bandwidth use because RBSCP tells the SCTP implementation at the end hosts to retransmit the dropped packets and this prevents the end hosts from assuming that the network is congested.
Step 12	**tunnel rbscp window-stuff** *step-size* **Example:** `Router(config-if)# tunnel rbscp window-stuff 1`	(Optional) Enables TCP window stuffing by increasing the value of the TCP window scale for RBSCP tunnels. • Use the *step-size* argument to specify the step increment number.

Step 13	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

What to Do Next

This task must be repeated on the router on the other side of the satellite link. Substitute the sample IP addresses, hostnames, and other parameters for the appropriate values on the second router.

After the task is completed on the router on the other side of the satellite link, proceed to the "Verifying RBSCP Tunnel Configuration and Operation" section on page 735.

Verifying Tunnel Configuration and Operation

This optional task explains how to verify tunnel configuration and operation. The commands contained in the task steps can be used in any sequence and may need to be repeated. The following commands can be used for GRE tunnels, IPv6 manually configured tunnels, and IPv6 over IPv4 GRE tunnels.

SUMMARY STEPS

1. **enable**
2. **show interfaces tunnel** *number* [**accounting**]
3. **ping** [*protocol*] *destination*

4. **show ip route** [*address* [*mask*]]
5. **ping** [*protocol*] *destination*

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show interfaces tunnel** *number* [**accounting**]

Assuming a generic example suitable for both IPv6 manually configured tunnels and IPv6 over IPv4 GRE tunnels, two routers are configured to be endpoints of a tunnel. Router A has Ethernet interface 0/0 configured as the source for tunnel interface 0 with an IPv4 address of 10.0.0.1 and an IPv6 prefix of 2001:0DB8:1111:2222::1/64. Router B has Ethernet interface 0/0 configured as the source for tunnel interface 1 with an IPv4 address of 10.0.0.2 and an IPv6 prefix of 2001:0DB8:1111:2222::2/64.

To verify that the tunnel source and destination addresses are configured, use the **show interfaces tunnel** command on Router A.

```
RouterA# show interfaces tunnel 0

Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.1 (Ethernet0/0), destination 10.0.0.2, fastswitch TTL 255
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled,  fast tunneling enabled
  Last input 00:00:14, output 00:00:04, 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: fifo
  Output queue :0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4 packets input, 352 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
     8 packets output, 704 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Step 3 **ping** [*protocol*] *destination*

To check that the local endpoint is configured and working, use the **ping** command on Router A.

```
RouterA# ping 2001:0DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0DB8:1111:2222::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

Step 4 **show ip route** [*address* [*mask*]]

To check that a route exists to the remote endpoint address, use the **show ip route** command.

```
RouterA# show ip route 10.0.0.2

Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Ethernet0/0
      Route metric is 0, traffic share count is 1
```

Step 5 **ping** [*protocol*] *destination*

To check that the remote endpoint address is reachable, use the **ping** command on Router A.

Note The remote endpoint address may not be reachable using the **ping** command because of filtering, but the tunnel traffic may still reach its destination.

```
RouterA# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/28 ms
```

To check that the remote IPv6 tunnel endpoint is reachable, use the **ping** command again on Router A. The same note on filtering also applies to this example.

```
RouterA# ping 1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

These steps may be repeated at the other endpoint of the tunnel.

Verifying RBSCP Tunnel Configuration and Operation

Perform one or both of the following optional tasks to verify the configuration and operation of the RBSCP tunnel configured in the "Configuring the RBSCP Tunnel" section on page 731.

- Verifying That the RBSCP Tunnel Is Active, page 735
- Verifying the RBSCP Traffic, page 737

Verifying That the RBSCP Tunnel Is Active

Perform this task to verify that the RBSCP tunnel is active.

SUMMARY STEPS

1. **enable**
2. **show rbscp** [**all** | **state** | **statistics**] [**tunnel** *tunnel-number*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show rbscp** [**all** | **state** | **statistics**] [**tunnel** *tunnel-number*]

Use this command with the **state** and **tunnel** keywords to display information about the current state of the tunnel. In the following sample output the tunnel is shown in an open state.

```
Router# show rbscp state tunnel 1

Tunnel1 is up, line protocol is up
RBSCP operational state:  OPEN
RBSCP operating mode: (264h) ack-split window-stuffing inorder SCTP-report
 window step: 1
 drop scale: 0
 ACK split size: 4
 input drop scale: 2
 initial TSN: 1h
 fuzz factor: 0
 max burst: tunnel 0, network 0
 next TSN: 1h
 next sequence: 16Bh
 current outstanding: 0
 max out per RTT: 2062500
 packets since SACK: 0
 cumulative ack: 0h
 TSN at SACK: 0h
 last cumulative ack: 0h
 last delivered TSN: 0h
 next FWDTSN corr: 0h
 RTO: 704 ms
 RTT: 550 ms     srtt_sa: 4391   srtt_sv: 3
 sentQ: num packets: 0, num bytes: 0
 tmitQ: num packets: 0, num bytes: 0
```

Use this command with the **statistics** and **tunnel** keywords to display statistical information about the tunnel. All counters display totals accumulated since the last **clear rbscp** command was issued.

```
Router# show rbscp statistics tunnel 0

Tunnel0 is up, line protocol is up
RBSCP protocol statistics:
 Init FWD-TSNs sent 0, received 0
 TUNNEL-UPs sent 0, received 0
 CLOSEDs sent 0, received 0
 TSNs sent 0, resent 0, lost by sender 0
 TSNs received 0 (duplicates 0)
 FWD-TSNs sent 144 (heartbeats 0)
 FWD-TSNs received 0 (ignored 0)
 FWD-TSNs caused 0 packet drops, 0 whole window drops
 SACKs sent 0, received 0 (ignored 0)
 Recovered with RTX 0
 Received with delay 0
 Most released at once 0
 Failed sends into the: tunnel 1, network 0
 Dropped due to: excess delay 0, tmit queue full 0
 Max on any queue: num packets: 0, num bytes: 0
 Max outstanding: 0
```

Verifying the RBSCP Traffic

Perform this task to verify that the traffic is being transmitted through the RBSCP tunnel and across the satellite link.

SUMMARY STEPS

1. **enable**
2. **show interfaces tunnel** *number* [**accounting**]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show interfaces tunnel** *number* [**accounting**]

Use this command to show that traffic is being transmitted through the RBSCP tunnel.

```
Router# show interfaces tunnel 0

Tunnel0 is up, line protocol is down
 Hardware is Tunnel
 Internet address is 172.17.1.4/24
 MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation TUNNEL, loopback not set
 Keepalive not set
 Tunnel source 172.17.1.2, destination 172.20.1.3
 Tunnel protocol/transport RBSCP/IP, key disabled, sequencing disabled
 Tunnel TTL 255
 Checksumming of packets disabled
 Tunnel transmit bandwidth 1000 (kbps)
 Tunnel receive bandwidth 8000 (kbps)
RBSCP operational state:  invalid (0h)
RBSCP operating mode: (2EEh) delay dual-delay drop-long-delay ack-split window-t
 window step: 3
 drop scale : 0
 ACK split size: 6
 input drop scale: 5
 initial TSN: 1h
 fuzz factor: 0
 next TSN: 1h
 next sequence: 1h
 current outstanding: 0
 max out per RTT: 550000
 packets since SACK: 0
 cumulative ack: 0h
 TSN at SACK: 1h
 last cumulative ack: 0h
 last delivered TSN: 0h
 next FWDTSN corr: 0h
 RTO: 704 ms
 RTT: 550 ms     srtt_sa: 0      srtt_sv: 4
 sentQ: num packets: 0, num bytes: 0
 tmitQ: num packets: 0, num bytes: 0

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: fifo
 Output queue: 0/0 (size/max)
 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, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Configuration Examples for Implementing Tunnels

This section contains the following examples:

- Configuring GRE/IPv4 Tunnels: Examples, page 738
- Configuring GRE/IPv6 Tunnels: Example, page 740
- Routing Two AppleTalk Networks Across an IP-Only Backbone: Example, page 740
- Routing a Private IP Network and a Novell Network Across a Public Service Provider: Example, page 741
- Configuring a CTunnel: Example, page 743
- Configuring GRE/CLNS CTunnels to Carry IPv4 and IPv6 Packets: Examples, page 744
- Configuring Manual IPv6 Tunnels: Example, page 746
- Configuring 6to4 Tunnels: Example, page 746
- Configuring IPv4-Compatible IPv6 Tunnels: Example, page 747
- Configuring ISATAP Tunnels: Example, page 747
- Configuring the RBSCP Tunnel: Example, page 747
- Configuring Routing for the RBSCP Tunnel: Example, page 748
- Configuring QoS Options on Tunnel Interfaces: Examples, page 750

Configuring GRE/IPv4 Tunnels: Examples

The following example shows a simple configuration of GRE tunneling. Note that Ethernet interface 0/1 is the tunnel source for Router A and the tunnel destination for Router B. Fast Ethernet interface 0/1 is the tunnel source for Router B and the tunnel destination for Router A.

Router A

```
interface Tunnel0
 ip address 10.1.1.2 255.255.255.0
 tunnel source Ethernet0/1
 tunnel destination 192.168.3.2
 tunnel mode gre ip
!
interface Ethernet0/1
 ip address 192.168.4.2 255.255.255.0
```

Router B

```
interface Tunnel0
 ip address 10.1.1.1 255.255.255.0
 tunnel source FastEthernet0/1
 tunnel destination 192.168.4.2
 tunnel mode gre ip
!
interface FastEthernet0/1
 ip address 192.168.3.2 255.255.255.0
```

The following example configures a GRE tunnel running both IS-IS and IPv6 traffic between Router A and Router B.

Router A

```
ipv6 unicast-routing
clns routing
!
interface Tunnel0
 no ip address
 ipv6 address 2001:0DB8:1111:2222::1/64
 ipv6 router isis
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.2
 tunnel mode gre ip
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
!
router isis
 network 49.0000.0000.000a.00
```

Router B

```
ipv6 unicast-routing
clns routing
!
interface Tunnel0
 no ip address
 ipv6 address 2001:0DB8:1111:2222::2/64
 ipv6 router isis
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.1
 tunnel mode gre ip
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
router isis
 network 49.0000.0000.000b.00
 address-family ipv6
 redistribute static
 exit-address-family
```

Configuring GRE/IPv6 Tunnels: Example

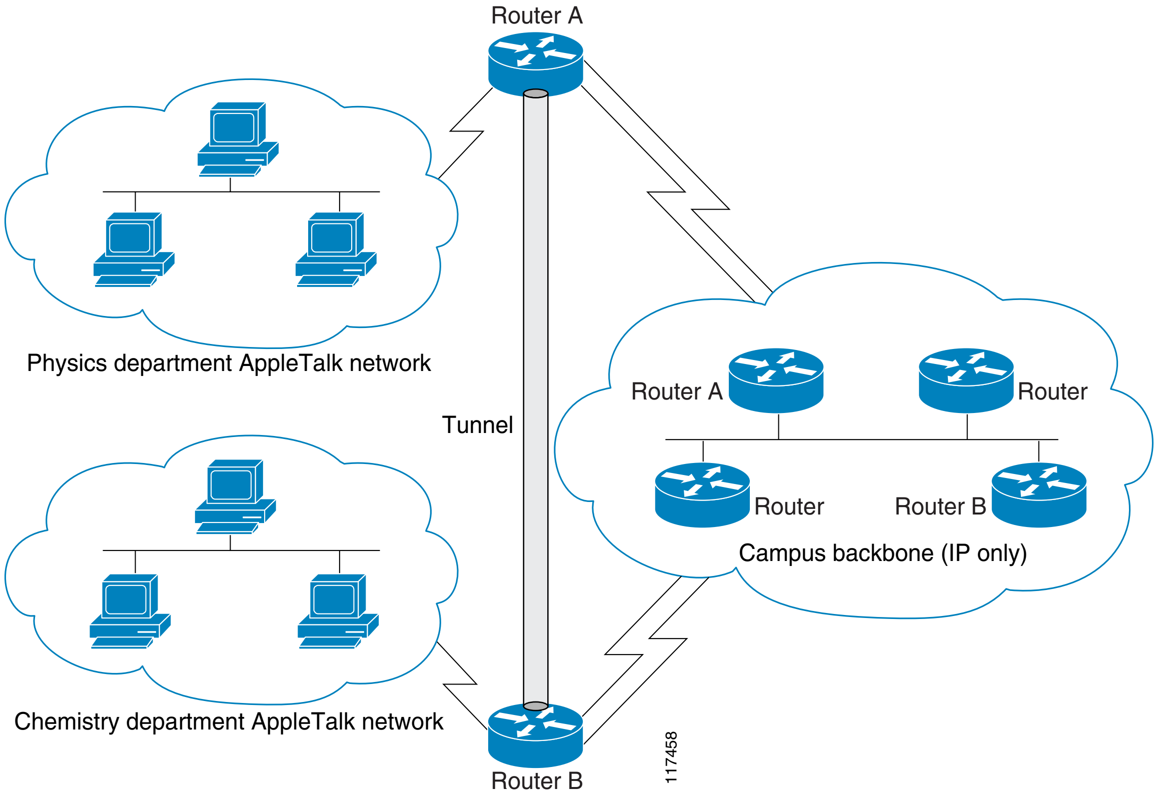
The following example shows how to configure a GRE tunnel over an IPv6 transport. Ethernet0/0 has an IPv6 address configured, and this is the source address used by the tunnel interface. The destination IPv6 address of the tunnel is specified directly. In this example, the tunnel carries both IPv4 and IS-IS traffic:

```
interface Tunnel0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
 tunnel source Ethernet0/0
 tunnel destination 2001:DB8:1111:2222::1
 tunnel mode gre ipv6
!
interface Ethernet0/0
 no ip address
 ipv6 address 2001:DB8:1111:1111::1/64
!
router isis
 net 49.0001.0000.0000.000a.00
```

Routing Two AppleTalk Networks Across an IP-Only Backbone: Example

Figure 73 is an example of connecting multiprotocol subnetworks across a single-protocol backbone. The configurations of Router A and Router B follow Figure 73.

Figure 73 Connecting AppleTalk Networks Across an IP-Only Backbone


Router A
Physics department AppleTalk network
Tunnel
Router A
Router
Router
Router B
Campus backbone (IP only)
Chemistry department AppleTalk network
Router B
117458

Router A

```
interface ethernet 0
 description physics department AppleTalk LAN
 appletalk cable-range 4001-4001 32
 !
interface fddi 0
 description connection to campus backbone
 ip address 10.0.8.108 255.255.255.0
interface tunnel 0
 tunnel source fddi 0
 tunnel destination 10.0.21.20
 appletalk cable-range 5313-5313 1
```

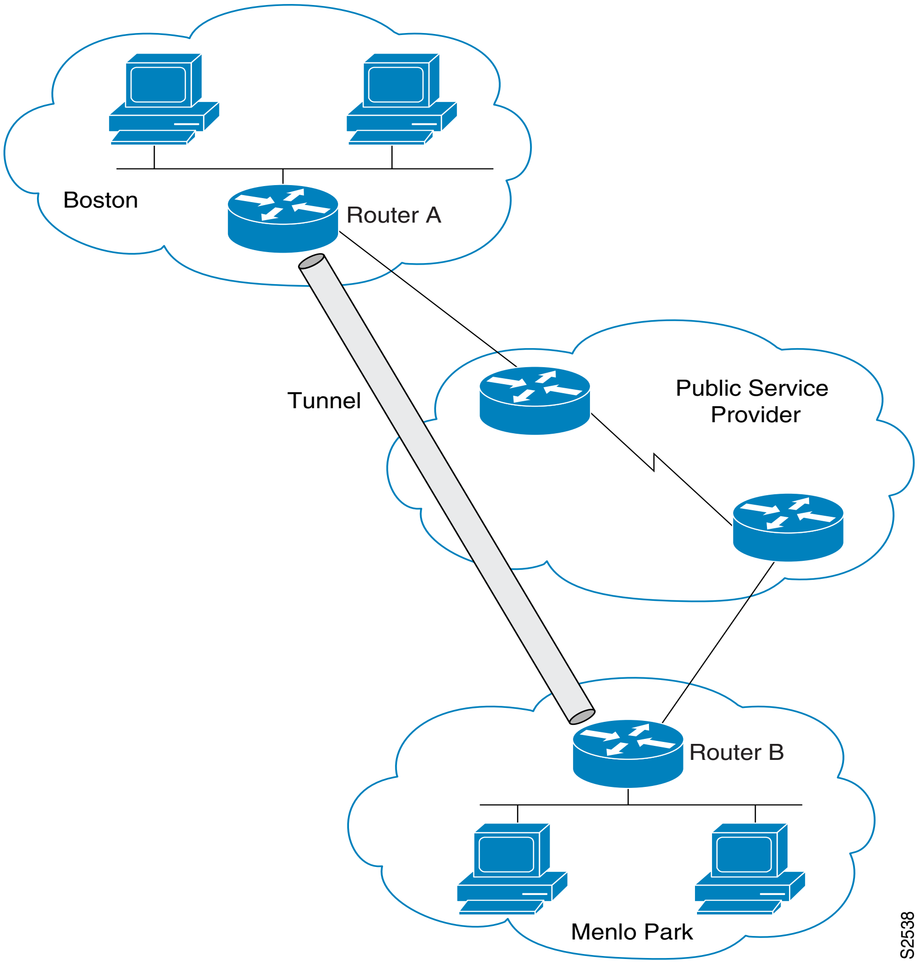
Router B

```
interface ethernet 0
 description chemistry department AppleTalk LAN
 appletalk cable-range 9458-9458 3
 !
interface fddi 0
 description connection to campus backbone
 ip address 10.0.21.20 255.255.255.0
interface tunnel 0
 tunnel source fddi 0
 tunnel destination 10.0.8.108
 appletalk cable-range 5313-5313 2
```

Routing a Private IP Network and a Novell Network Across a Public Service Provider: Example

Figure 74 is an example of routing a private IP network and a Novell network across a public service provider. The configurations of Router A and Router B follow Figure 74.

Figure 74 Creating Virtual Private Networks Across WANs



Router A

```
interface ethernet 0
 description Boston office
 ip address 10.1.1.1 255.255.255.0
 novell network 1e
!
interface serial 0
 description connection to public service provider
 ip address 172.17.2.1 255.255.255.0
!
interface tunnel 0
 tunnel source serial 0
 tunnel destination 172.28.5.2
 ip address 10.1.2.1 255.255.255.0
 novell network 1f
```

Router B

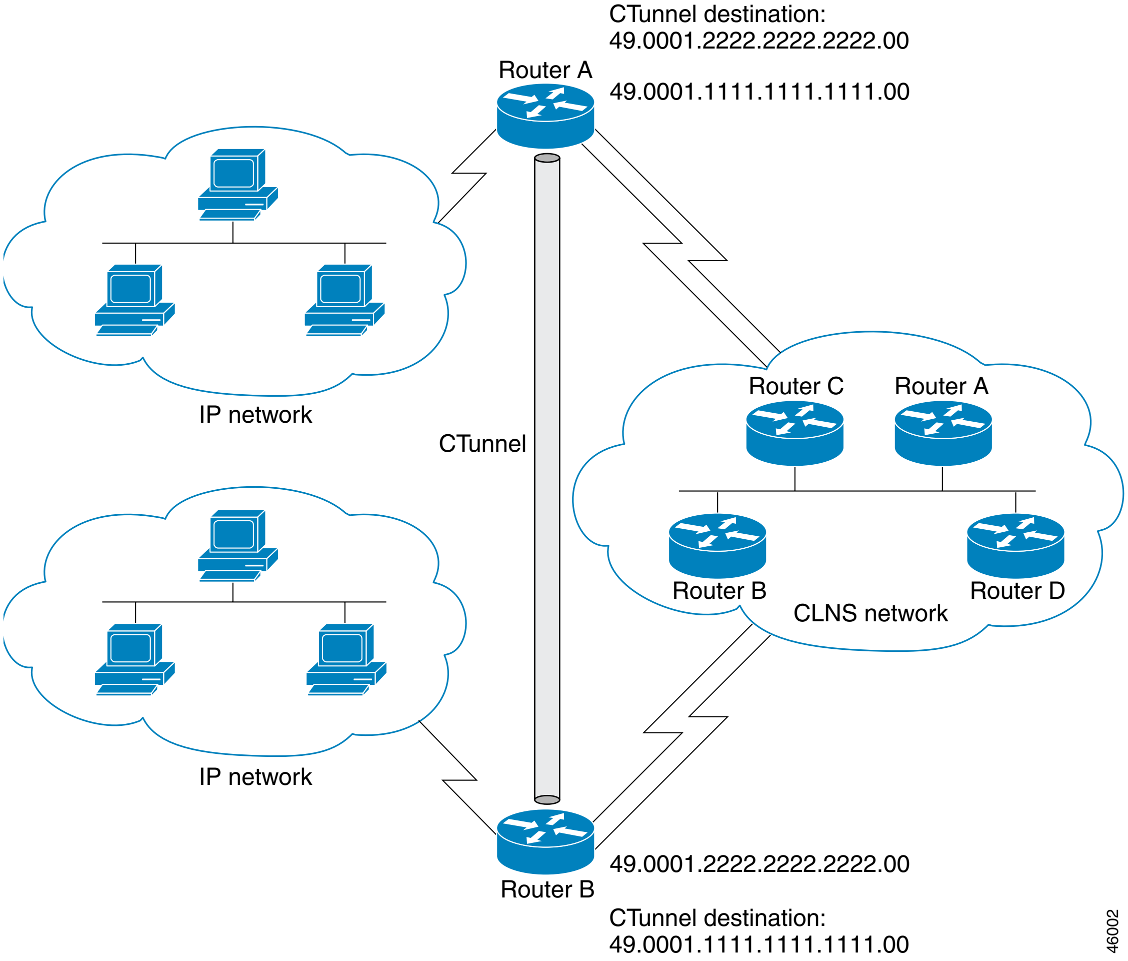
```
interface ethernet 0
 description Menlo Park office
 ip address 10.1.3.1 255.255.255.0
 novell network 31
 !
```

```
interface serial 4
 description connection to public service provider
 ip address 172.28.5.2 255.255.255.0
 !
interface tunnel 0
 tunnel source serial 4
 tunnel destination 172.17.2.1
 ip address 10.1.2.2 255.255.255.0
 novell network 1f
```

Configuring a CTunnel: Example

Figure 75 illustrates the creation of a CTunnel between Router A and Router B, as accomplished in the configuration examples that follow.

Figure 75 Creation of a CTunnel



Router A

```
ip routing
clns routing

interface ctunnel 102
 ip address 10.0.0.1 255.255.255.0
 ctunnel destination 49.0001.2222.2222.2222.00

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.1111.1111.1111.00
router rip
 network 10.0.0.0
```

Router B

```
ip routing
clns routing

interface ctunnel 201
 ip address 10.0.0.2 255.255.255.0
 ctunnel destination 49.0001.1111.1111.1111.00

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.2222.2222.2222.00

router rip
 network 10.0.0.0
```

Configuring GRE/CLNS CTunnels to Carry IPv4 and IPv6 Packets: Examples

The following example configures a GRE CTunnel running both IS-IS and IPv6 traffic between Router A and Router B in a CLNS network. The **ctunnel mode gre** command provides a method of tunneling that is compliant with RFC 3147 and should allow tunneling between Cisco equipment and third-party networking devices.

Router A

```
ipv6 unicast-routing

clns routing

interface ctunnel 102
 ipv6 address 2001:0DB8:1111:2222::1/64
 ctunnel destination 49.0001.2222.2222.2222.00
 ctunnel mode gre

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.1111.1111.1111.00
```

Router B

```
ipv6 unicast-routing

clns routing

interface ctunnel 201
 ipv6 address 2001:0DB8:1111:2222::2/64
 ctunnel destination 49.0001.1111.1111.1111.00
 ctunnel mode gre

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.2222.2222.2222.00
```

To turn off GRE mode and restore the CTunnel to the default Cisco encapsulation routing only between endpoints on Cisco equipment, use either the **no ctunnel mode** command or the **ctunnel mode cisco** command. The following example shows the same configuration modified to transport only IPv4 traffic.

Router A

```
ip routing

clns routing

interface ctunnel 102
 ip address 10.2.2.5 255.255.255.0
 ctunnel destination 49.0001.2222.2222.2222.00
 ctunnel mode cisco

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.1111.1111.1111.00
```

Router B

```
ip routing

clns routing

interface ctunnel 201
 ip address 10.0.0.5 255.255.255.0
 ctunnel destination 49.0001.1111.1111.1111.00
 ctunnel mode cisco

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.2222.2222.2222.00
```

Configuring Manual IPv6 Tunnels: Example

The following example configures a manual IPv6 tunnel between Router A and Router B. In the example, tunnel interface 0 for both Router A and Router B is manually configured with a global IPv6 address. The tunnel source and destination addresses are also manually configured.

Router A

```
interface ethernet 0
 ip address 192.168.99.1 255.255.255.0

interface tunnel 0
 ipv6 address 2001:0db8:c18:1::3/126
 tunnel source ethernet 0
 tunnel destination 192.168.30.1
 tunnel mode ipv6ip
```

Router B

```
interface ethernet 0
 ip address 192.168.30.1 255.255.255.0

interface tunnel 0
 ipv6 address 2001:0db8:c18:1::2/126
 tunnel source ethernet 0
 tunnel destination 192.168.99.1
 tunnel mode ipv6ip
```

Configuring 6to4 Tunnels: Example

The following example configures a 6to4 tunnel on a border router in an isolated IPv6 network. The IPv4 address is 192.168.99.1, which translates to the IPv6 prefix of 2002:c0a8:6301::/48. The IPv6 prefix is subnetted into 2002:c0a8:6301::/64 for the tunnel interface: 2002:c0a8:6301:1::/64 for the first IPv6 network and 2002:c0a8:6301:2::/64 for the second IPv6 network. The static route ensures that any other traffic for the IPv6 prefix 2002::/16 is directed to tunnel interface 0 for automatic tunneling.

```
interface Ethernet0
 description IPv4 uplink
 ip address 192.168.99.1 255.255.255.0
!
interface Ethernet1
 description IPv6 local network 1
 ipv6 address 2002:c0a8:6301:1::1/64
!
interface Ethernet2
 description IPv6 local network 2
 ipv6 address 2002:c0a8:6301:2::1/64
!
interface Tunnel0
 description IPv6 uplink
 no ip address
 ipv6 address 2002:c0a8:6301::1/64
 tunnel source Ethernet0
 tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 Tunnel0
```

Configuring IPv4-Compatible IPv6 Tunnels: Example

The following example configures an IPv4-compatible IPv6 tunnel that allows BGP to run between a number of routers without having to configure a mesh of manual tunnels. Each router has a single IPv4-compatible tunnel, and multiple BGP sessions can run over each tunnel, one to each neighbor. Ethernet interface 0 is used as the tunnel source. The tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of an IPv4-compatible IPv6 address. Specifically, the IPv6 prefix 0:0:0:0:0:0 is concatenated to an IPv4 address (in the format 0:0:0:0:0:0:A.B.C.D or ::A.B.C.D) to create the IPv4-compatible IPv6 address. Ethernet interface 0 is configured with a global IPv6 address and an IPv4 address (the interface supports both the IPv6 and IPv4 protocol stacks).

Multiprotocol BGP is used in the example to exchange IPv6 reachability information with the peer 10.67.0.2. The IPv4 address of Ethernet interface 0 is used in the low-order 32 bits of an IPv4-compatible IPv6 address and is also used as the next-hop attribute. Using an IPv4-compatible IPv6 address for the BGP neighbor allows the IPv6 BGP session to be automatically transported over an IPv4-compatible tunnel.

```
interface tunnel 0
 tunnel source Ethernet 0
 tunnel mode ipv6ip auto-tunnel

interface ethernet 0
 ip address 10.27.0.1 255.255.255.0
 ipv6 address 3000:2222::1/64

router bgp 65000
 no synchronization
 no bgp default ipv4-unicast
 neighbor ::10.67.0.2 remote-as 65002

address-family ipv6
 neighbor ::10.67.0.2 activate
 neighbor ::10.67.0.2 next-hop-self
 network 2001:2222:d00d:b10b::/64
```

Configuring ISATAP Tunnels: Example

The following example shows the tunnel source defined on Ethernet 0 and the **tunnel mode** command used to configure the ISATAP tunnel. Router advertisements are enabled to allow client autoconfiguration.

```
interface Tunnel1
 tunnel source ethernet 0
 tunnel mode ipv6ip isatap
 ipv6 address 2001:0DB8::/64 eui-64
 no ipv6 nd suppress-ra
```

Configuring the RBSCP Tunnel: Example

In the following example, Router 1 and Router 2 are configured to send traffic through an RBSCP tunnel over a satellite link.

Router 1

```
interface Tunnel 0
 ip unnumbered ethernet1
 tunnel source ethernet1
 tunnel destination 172.17.2.1
 tunnel bandwidth transmit 1000
 tunnel mode rbscp
 tunnel rbscp ack-split 6
 tunnel rbscp report
!
interface ethernet1
 description Satellite Link
 ip address 172.20.1.2 255.255.255.0
```

Router 2

```
interface Tunnel 0
 ip unnumbered ethernet1
 tunnel source ethernet1
 tunnel destination 172.20.1.2
 tunnel bandwidth transmit 1000
 tunnel mode rbscp
 tunnel rbscp ack-split 6
 tunnel rbscp report
!
interface ethernet1
 description Satellite Link
 ip address 172.17.2.1 255.255.255.0
```

Configuring Routing for the RBSCP Tunnel: Example

To control the type of traffic that uses the RBSCP tunnel, you must configure the appropriate routing. If you want to direct all traffic through the tunnel, you can configure a static route.

Note To prevent routing flaps, remember to configure the tunnel interface as passive if dynamic routing protocols are used.

The following example shows how to use policy-based routing to route some specific protocol types through the tunnel. In this example, an extended access list allows TCP, Stream Control Transmission Protocol (SCTP), Encapsulating Security Payload (ESP) protocol, and Authentication Header (AH) traffic to travel through the tunnel. All IP traffic is denied.

Router 1 (Local Side)

```
interface Tunnel1
 ip unnumbered FastEthernet1/1
 tunnel source FastEthernet1/1
 tunnel destination 10.12.0.20
 tunnel mode rbscp
 tunnel ttl 5
 tunnel bandwidth transmit 30000
 tunnel rbscp window-stuff 1
 tunnel rbscp ack-split 4
!
interface FastEthernet0/0
 ip address 10.13.0.1 255.255.255.0
 ip policy route-map rbscp-pbr
 duplex auto
 speed auto
!
interface FastEthernet1/1
 description Satellite Link
 ip address 10.12.0.1 255.255.255.0
 duplex auto
 speed auto
!
ip route 10.15.0.0 255.255.255.0 FastEthernet1/1
!
ip access-list extended rbscp-acl
 permit tcp any 10.15.0.0 0.0.0.255
 permit 132 any 10.15.0.0 0.0.0.255
 permit esp any 10.15.0.0 0.0.0.255
 permit ahp any 10.15.0.0 0.0.0.255
 deny ip any any
!
route-map rbscp-pbr permit 10
 match ip address rbscp-acl
 set interface Tunnel1
```

Router 2 (Remote Side)

```
ip dhcp pool CLIENT
 import all
 network 10.15.0.0 255.255.255.0
 default-router 10.15.0.1
 domain-name engineer.chicago.il.us
 dns-server 10.10.0.252
!
interface Tunnel1
 ip unnumbered FastEthernet0/1
 tunnel source FastEthernet0/1
 tunnel destination 10.12.0.1
 tunnel mode rbscp
 tunnel ttl 5
 tunnel bandwidth transmit 30000
 tunnel rbscp window-stuff 1
 tunnel rbscp ack-split 4
!
interface FastEthernet0/0
 description Local LAN
 ip address 10.15.0.1 255.255.255.0
 ip policy route-map rbscp-pbr
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description Satellite Link
 ip address 10.12.0.20 255.255.255.0
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
ip access-list extended rbscp-acl
 permit tcp any any
 permit 132 any any
 permit esp any any
 permit ahp any any
 deny ip any any
!
route-map rbscp-pbr permit 10
 match ip address rbscp-acl
 set interface Tunnel1
```

Configuring QoS Options on Tunnel Interfaces: Examples

The following sample configuration applies generic traffic shaping (GTS) directly on the tunnel interface. In this example the configuration shapes the tunnel interface to an overall output rate of 500 kbps. For more details on GTS, see the "Regulating Packet Flow Using Traffic Shaping" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.4.

```
interface Tunnel0
 ip address 10.1.2.1 255.255.255.0
 traffic-shape rate 500000 125000 125000 1000
 tunnel source 10.1.1.1
 tunnel destination 10.2.2.2
```

The following sample configuration shows how to apply the same shaping policy to the tunnel interface with the Modular QoS CLI (MQC) commands. For more details on MQC, see the "Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.4.

```
policy-map tunnel
 class class-default
 shape average 500000 125000 125000
!
interface Tunnel0
 ip address 10.1.2.1 255.255.255.0
 service-policy output tunnel
 tunnel source 10.1.35.1
 tunnel destination 10.1.35.2
```

Policing Example

When an interface becomes congested and packets start to queue, you can apply a queueing method to packets that are waiting to be transmitted. Cisco IOS logical interfaces—tunnel interfaces in this example—do not inherently support a state of congestion and do not support the direct application of a service policy that applies a queueing method. Instead, you need to apply a hierarchical policy. Create a "child" or lower-level policy that configures a queueing mechanism, such as low latency queueing with the **priority** command and class-based weighted fair queueing (CBWFQ) with the **bandwidth** command.

```
policy-map child
 class voice
 priority 512
```

Create a "parent" or top-level policy that applies class-based shaping. Apply the child policy as a command under the parent policy because admission control for the child class is done according to the shaping rate for the parent class.

```
policy-map tunnel
 class class-default
 shape average 2000000
 service-policy child
```

Apply the parent policy to the tunnel interface.

```
interface tunnel0
 service-policy tunnel
```

In the following example, a tunnel interface is configured with a service policy that applies queueing without shaping. A log message is displayed noting that this configuration is not supported.

```
interface tunnel1
 service-policy output child
 Class Based Weighted Fair Queueing not supported on this interface
```

For more details on QoS policing, see the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4.

Where to Go Next

If you have implemented IPv6 tunnels, you may want to proceed to one of the following modules:

- If you have configured an automatic 6to4 tunnel, you can design your IPv6 network around the /48 6to4 prefix that you have created from your IPv4 address.
- If you want to implement routing protocols, see the "Implementing RIP for IPv6," "Implementing IS-IS for IPv6," "Implementing OSPF for IPv6," or "Implementing Multiprotocol BGP for IPv6" modules.
- If you want to implement security features for your IPv6 network, see the "Implementing Security for IPv6" module.

Additional References

- The following sections provide references related to implementing tunnels.

Related Documents

Related Topic	Document Title
Tunnel commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4
CLNS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS ISO CLNS Command Reference*, Release 12.4
IP commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	• *Cisco IOS IP Addressing Services Command Reference*, Release 12.4. • *Cisco IOS IP Application Services Command Reference*, Release 12.4. • *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4.
IPv6 commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IPv6 Command Reference*, Release 12.4
IPv6 configuration modules	*Cisco IOS IPv6 Configuration Library*, Release 12.4
QoS policing and generic traffic shaping configuration	"Policing and Shaping Overview" module in the *Cisco IOS Quality of Service Solutions Configuration Guide,* Release 12.4
Modular QoS CLI configuration	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4

Related Topic	Document Title
Virtual interface configuration	"Configuring Virtual Interfaces" module in the *Cisco IOS Interface and Hardware Component Configuration Guide,* Release 12.4
Configuration example for GRE over IP Security (IPSec) where the GRE/IPSec tunnel is going through a firewall doing Network Address Translation (NAT)	*Configuring IPSec/GRE with NAT*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been 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

RFC	Title
RFC 791	*Internet Protocol*
RFC 1191	*Path MTU Discovery*
RFC 1323	*TCP Extensions for High Performance*
RFC 1483	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*
RFC 2003	*IP Encapsulation Within IP*
RFC 2018	*TCP Selective Acknowledgment Options*
RFC 2460	*Internet Protocol, Version 6 (IPv6)*
RFC 2473	*Generic Packet Tunneling in IPv6 Specification*
RFC 2474	*Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*
RFC 2547	*BGP/MPLS VPNs*
RFC 2780	*IANA Allocation Guidelines for Values in the Internet Protocol and Related Headers*
RFC 2784	*Generic Routing Encapsulation (GRE)*
RFC 2890	*Key and Sequence Number Extensions to GRE*

RFC	Title
RFC 2893	*Transition Mechanisms for IPv6 Hosts and Routers*
RFC 3056	*Connection of IPv6 Domains via IPv4 Clouds*
RFC 3147	*Generic Routing Encapsulation over CLNS Networks*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of 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/techsupport

Feature Information for Implementing Tunnels

Table 46 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. 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.

Note Table 46 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 46 Feature Information for Implementing Tunnels

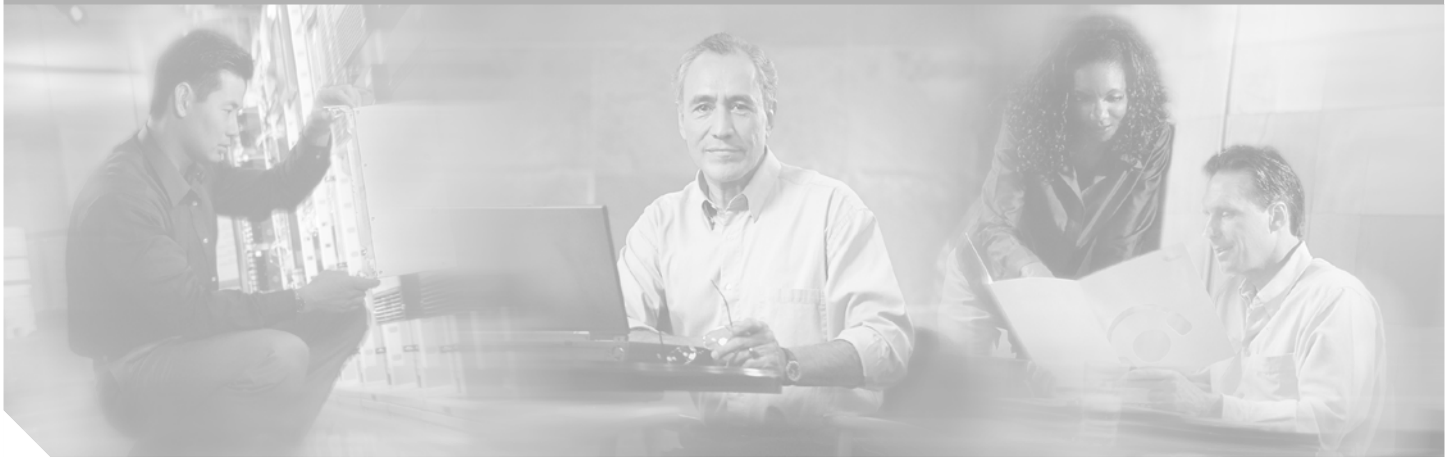
Feature Name	Releases	Feature Configuration Information
CEF-Switched Multipoint GRE Tunnels	12.2(8)T	The CEF-Switched Multipoint GRE Tunnels feature enables CEF switching of IP traffic to and from multipoint GRE tunnels. Tunnel traffic can be forwarded to a prefix through a tunnel destination when both the prefix and the tunnel destination are specified by the application. This feature introduces CEF switching over multipoint GRE tunnels. Previously, only process switching was available for multipoint GRE tunnels. The following sections provide information about this feature: • Multipoint GRE Tunneling, page 705 • Determining the Tunnel Type, page 714 • Configuring a GRE Tunnel, page 716 No commands were introduced or modified by this feature.

Table 46 Feature Information for Implementing Tunnels (continued)

Feature Name	Releases	Feature Configuration Information
CLNS Support for GRE Tunneling of IPv4 and IPv6 Packets in CLNS Networks	12.3(7)T 12.2(25)S	Support of the GRE tunnel mode allows Cisco CTunnels to transport IPv4 and IPv6 packets over CLNS-only networks in a manner that allows interoperation between Cisco networking equipment and that of other vendors. This feature provides compliance with RFC 3147. The following sections provide information about this feature: • GRE/CLNS Tunnel Support for IPv4 and IPv6 Packets, page 705 • Determining the Tunnel Type, page 714 • Configuring GRE/CLNS CTunnels to Carry IPv4 and IPv6 Packets, page 722 • Verifying Tunnel Configuration and Operation, page 733 The following command was introduced by this feature: **ctunnel mode**.
GRE Tunnel Keepalive	12.2(8)T 12.0(23)S	The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated generic routing encapsulation (GRE) tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side. The following section provides information about this feature: • Configuring a GRE Tunnel, page 716 The following command was introduced by this feature: **keepalive** (tunnel interfaces).

Table 46 Feature Information for Implementing Tunnels (continued)

Feature Name	Releases	Feature Configuration Information
Rate-Based Satellite Control Protocol	12.3(7)T	Rate-Based Satellite Control Protocol (RBSCP) was designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IP Security (IPSec), over satellite links without breaking the end-to-end model. The following sections provide information about this feature: • Rate-Based Satellite Control Protocol Tunnels, page 710 • Determining the Tunnel Type, page 714 • Configuring the RBSCP Tunnel, page 731 • Verifying RBSCP Tunnel Configuration and Operation, page 735 The following commands were introduced or modified by this feature: **clear rbscp**, **debug tunnel rbscp**, **show rbscp**, **tunnel bandwidth**, **tunnel mode**, **tunnel rbscp ack-split**, **tunnel rbscp delay**, **tunnel rbscp input-drop**, **tunnel rbscp long-drop**, **tunnel rbscp report**, **tunnel rbscp window-stuff**.
Tunnel ToS	12.0(17)S 12.0(17)ST 12.2(8)T 12.2(14)S	The Tunnel ToS feature allows you to configure the ToS and Time-to-Live (TTL) byte values in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. The Tunnel ToS feature is supported on Cisco Express Forwarding (CEF), fast switching, and process switching forwarding modes. The following section provides information about this feature: • Tunnel ToS, page 703 The following commands were introduced or modified by this feature: **show interfaces tunnel**, **tunnel tos**, **tunnel ttl**.



Part 5: Dial Shelves

Managing Dial Shelves

This chapter discusses configuration and monitoring tasks for dial shelves and dial shelf controllers, particularly on Cisco AS5800 Universal Access Servers.

To identify the hardware platform or software image information associated with a feature, use Cisco Feature Navigator on Cisco.com to search for information about the feature.

For additional information about the technologies in this chapter, see the following publications:

- *Dial and System Management Commands for the Cisco AS5800*
  (This document is available online only.)
- *Cisco AS5800 Access Server Software ICG*
- *Cisco IOS Dial Technologies Configuration Guide* and *Cisco IOS Dial Technologies Command Reference* (Release 12.2)

For hardware technical descriptions and information about installing interfaces, refer to the hardware installation and configuration publication for your product. For a complete description of dial shelf management commands in this chapter, refer to the *Cisco IOS Interface and Hardware Component Command Reference*. To locate documentation of other commands that appear in this chapter, use the master commands list or search online.

Dial Shelf Management Task List

To manage dial shelves, perform the tasks in the following sections:

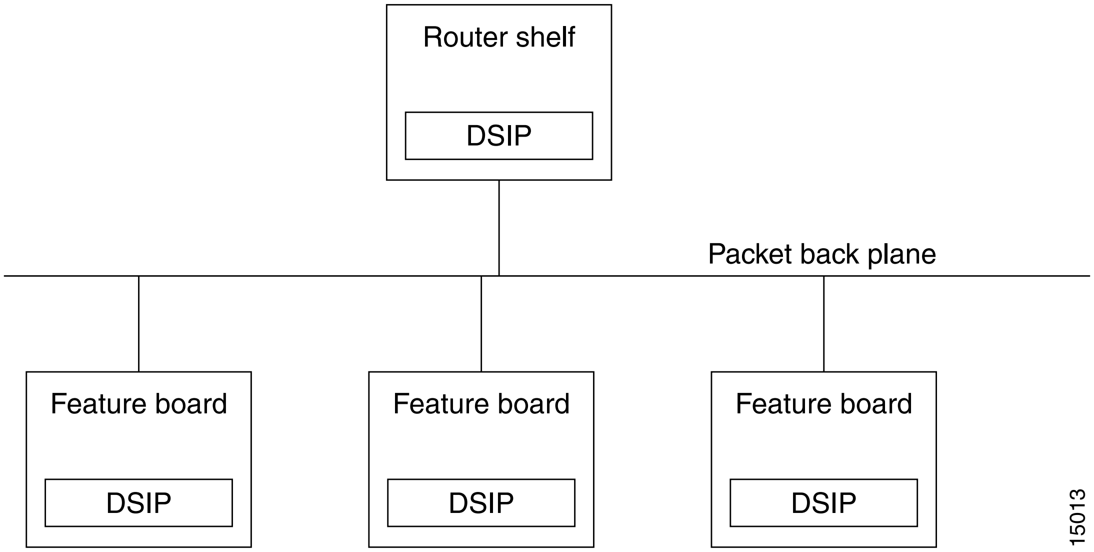
- Understanding Shelf Architecture and DSIP, page 759
- Maintaining Shelves, page 760
- Maintaining Dial Shelf Controllers, page 762
- Troubleshooting Using DSIP, page 764

Understanding Shelf Architecture and DSIP

The Cisco AS5800 is a rack-mounted system consisting of a router shelf and a dial shelf. The dial shelf contains trunk cards, modem cards, and dial shelf controller (DSC) cards. The trunk cards and modem cards are referred to collectively as feature boards. Slots 0 through 11 of the dial shelf are reserved for feature boards, while slots 12 and 13 are reserved for the DSC cards. The AS5800 series supports the use of a single router shelf or two router shelves (split-shelf configuration), and the use of a single DSC or two DSCs (DSC redundancy) for backup purposes.

Dial Shelf Interconnect Protocol (DSIP) is used for communication between router shelf and dial shelf on an AS5800. Figure 76 diagrams the components of the architecture. DSIP communicates over the packet backplane via the dial shelf interconnect (DSI) cable.

Figure 76 DSIP Architecture in the Cisco AS5800



Maintaining Shelves

Perform the tasks described in the following sections to perform the respective configuration tasks:

- Configuring the Shelf IDs, page 760
- Executing Commands Remotely, page 762

Configuring the Shelf IDs

The Cisco AS5800 consists of one or more router shelves and a dial shelf. Shelf ID numbers and port numbers are used to identify specific components in your system. The default shelf number is 0 for the router shelf and 1 for the dial shelf.

Normally you do not need to change the shelf IDs; however, if you do, we recommend that you change the shelf number when you initially access the setup facility. For information on the setup facility, refer to the *Cisco AS5800 Universal Access Server Software Installation and Configuration Guide*.

Caution You must reload the Cisco AS5800 for the new shelf number to take effect. Because the shelf number is part of the interface names when you reload, all NVRAM interface configuration information is lost.

If you are booting the router shelf from the network (netbooting), you can change the shelf numbers using the **shelf-id** command. Perform the following steps beginning in EXEC mode.

	Command or Action	Purpose
Step 1	**copy startup-configure tftp**	Saves your current configuration. Changing the shelf number removes all interface configuration information when you reload the Cisco AS5800.
Step 2	**configure terminal**	Enters configuration mode.
Step 3	**shelf-id** *number* **router-shelf**	Specifies the router shelf ID.
Step 4	**shelf-id** *number* **dial-shelf**	Specifies the dial shelf ID.
Step 5	**exit**	Exits configuration mode.
Step 6	**copy running-config startup-config**	(Optional) Saves your configuration.
Step 7	**show version**	Verifies that the correct shelf number will be changed after the next reload.
Step 8	**reload**	Reloads the Cisco AS5800.
Step 9	Type "yes" to the "save config" prompt.	—
Step 10	Configure one interface so that router shelf has connectivity to the server with the configuration.	—
Step 11	**copy tftp startup-config**	Because changing the shelf number removes all interface configuration information when you reload the Cisco AS5800, edit the configuration file saved in Step 1 and download it.

If you are booting the router shelf from flash memory, perform the following steps beginning in EXEC mode.

	Command or Action	Purpose
Step 1	**copy running-config tftp** or **copy startup-config tftp**	Saves your current (latest) configuration to a server.
Step 2	**configure terminal**	Enters configuration mode.
Step 3	**shelf-id** *number* **router-shelf**	Configures the router shelf ID.
Step 4	**shelf-id** *number* **dial-shelf**	Configures the dial shelf ID.
Step 5	**exit**	Exits configuration mode.
Step 6	**copy running-config startup-config**	(Optional) Saves your configuration. If this step is skipped, type "No" to the 'save configuration' prompt.
Step 7	**show version**	Allows verification that the correct shelf number will be changed after the next reload.
Step 8	Edit the configuration file saved in Step 1.	—

	Command or Action	Purpose
Step 9	`copy tftp startup-config`	Copies the edited configuration to NVRAM on the Cisco AS5800.
Step 10	`reload`	Reloads the system.

Executing Commands Remotely

It is possible to connect directly to the system console interface on the DSC to execute dial shelf configuration commands, but this is not recommended. All commands necessary for dial shelf configuration, including show and debug tasks, can be executed remotely through the router console. A special command called **execute-on** is provided for this purpose. This command enables a special set of Exec mode commands to be executed on the router or the dial shelf. This command is a convenience that avoids connecting the console to the DSC. For a list of commands that you can execute using **execute-on**, see the complete command description in the *Cisco IOS Configuration Fundamentals Command Reference*.

To enter a command that you wish to execute on a specific card installed in the dial shelf while logged onto the router shelf console, use the following privileged EXEC mode commands.

Command	Purpose
execute-on slot *slot command*	Executes a command from the router shelf on a specific card in the dial shelf.
execute-on all *command*	Executes a command from the router shelf on all cards in the dial shelf.

Maintaining Dial Shelf Controllers

The DSC card provides the following:

- Master clock for the dial shelf
- Fast Ethernet link to the router shelf
- Environmental monitoring of the feature boards
- Bootstrap images on start-up for the feature boards

The Cisco AS5800 dial shelf can contain two DSC cards. With two DSC cards present, DSC redundancy automatically provides for one DSC to act as a backup to the active one. This redundancy feature is implemented to increase system availability by preventing loss of service in the event of the failure of one of the DSCs. The redundancy is intended to be transparent to most Cisco AS5800 software (redundancy is supported at or below the DSIP layer). Software modules using the DSIP services are generally not aware of nor need to take part in the management of dual DSCs.

Configuring Clocks

The TDM bus in the backplane on the dial shelf must be synchronized to the T1/E1 clocks on the trunk cards. The Dial Shelf Controller (DSC) card on the dial shelf provides hardware logic to accept multiple clock sources as input and use one of them as the primary source to generate a stable, PPL synchronized output clock. The input clock can be any of the following sources:

- Trunk port in slots 0 through 5—up to 12 can be selected (2 per slot)
- An external T1 or E1 clock source fed directly through a connector on the DSC card
- A free-running clock from an oscillator in the clocking hardware on the DSC card

For dual (redundant) DSC cards, the external DSC clocking port should be configured so that the clock signal fed into both DSCs is identical.

To configure the clock source and priority of the clock source used by the TDM bus, perform one or more of the following steps, beginning in global configuration mode.

	Command	Purpose
Step 1	**dial-tdm-clock priority** *number* **trunk-slot** *slot* **port** *number*	Configure the priority of the trunk card clock.
Step 2	**dial-tdm-clock priority** *number* **freerun**	Configure the priority of the free running clock.
Step 3	**dial-tdm-clock priority** *number* **external** {**e1** | **t1**} [**120ohm**]	Configure the priority of the T1 or E1 external clock.
Step 4	**exit**	Exit configuration mode.
Step 5	**copy running-config startup-config**	Save your configuration.
Step 6	**show dial-shelf clocks**	Verify the clocking priorities.

Monitoring and Maintaining DSCs and Feature Boards

Use the following commands in privileged EXEC mode to swap dial shelf cards or to troubleshoot the dial shelf cards from the router shelf.

Command	Purpose
hw-module slot *shelf-id***/***slot-number* {**start** | **stop**}	Stops a DSC remotely from the router console or restarts the DSC if it has been stopped.
hw-module slot *shelf-id***/***slot-number* **reload**	Reloads the specified feature board. This command can be used instead of a manual online insertion and removal (OIR) to reload and power-cycle a feature board. Note that this command cannot be applied to DSCs.
show redundancy [**history**]	Displays the current or history status for redundant DSC.
debug redundancy {**all** | **ui** | **clk** | **hub**}	Use this debug command if you need to collect events for troubleshooting, selecting the appropriate required key word.
show debugging	Lists the debug commands that are turned on, including that for redundant DSC.

Troubleshooting Using DSIP

There are a number of **show** commands available to aid in troubleshooting dial shelves. Use any of the following EXEC mode commands to monitor DSI and DSIP activity.

Command	Purpose
`clear dsip tracing`	Used to clear tracing statistics for the Distributed System Interconnect Protocol (DSIP).
`show dsip`	Displays all information about the Distributed System Interconnect Protocol (DSIP).
`show dsip clients`	Displays information about Distributed System Interconnect Protocol (DSIP) clients.
`show dsip nodes`	Displays information about the processors running the Distributed System Interconnect Protocol (DSIP).
`show dsip ports`	Displays information about local and remote ports.
`show dsip queue`	Displays the number of messages in the retransmit queue waiting for acknowledgment.
`show dsip tracing`	Displays Distributed System Interconnect Protocol (DSIP) tracing buffer information.
`show dsip transport`	Displays information about the Distributed System Interconnect Protocol (DSIP) transport statistics for the control/data and IPC packets and registered addresses.
`show dsip version`	Displays Distributed System Interconnect Protocol (DSIP) version information.

The privileged EXEC mode **show dsi** command can also be used to troubleshoot, as it displays the status of the DSI adapter, which is used to physically connect the router shelf and the dial shelf to enable DSIP communications.

The following is an example troubleshooting scenario:

Problem: The router shelf boots, but there is no communication between the router and dial shelves.

Step 1 Run the **show dsip transport** command.

Step 2 Check the "DSIP registered addresses" column. If there are zero entries here, there is some problem with the Dial Shelf Interconnect (DSI). Check if the DSI is installed in the router shelf.

Step 3 If there is only one entry and it is our own local address, then first sanity check the physical layer. Make sure that there is a physical connection between the RS and DS. If everything is fine from a cabling point of view, go to Step 4.

Step 4 Check the DSI health by issuing the **show dsi** command. This gives a consolidated output of DSI controller and interface. Check for any errors like runts, giants, throttles and other usual FE interface errors.

Diagnosis: If an entry for a particular dial shelf slot is not found among the registered addresses, but most of other card entries are present, the problem is most likely with that dial shelf slot. The DSI hardware on that feature board is probably bad.

Router-Shelf Redundancy for the Cisco AS5800

Feature History

Release	Modification
12.1(5) XV1	This feature was introduced.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the the Cisco AS5800 platform.

This document describes router-shelf redundancy for the Cisco AS5800 universal access server. It includes the following sections:

Feature Overview

This feature provides router-shelf redundancy by using a second router shelf that automatically takes over the other shelf’s dial-shelf cards (DSCs) if it appears that the other router shelf has died. Failover is disruptive in that there is no attempt to maintain calls that were established on the failing router shelf; the DSCs controlled by the failing router shelf are restarted under control of the backup router shelf and hence become available again.

Two router shelves are connected to the same DSC (as in split mode), but with only one router shelf active at a time. Both router shelves are configured for normal mode as opposed to split mode. Each router shelf contains the same configuration, being whatever configuration is appropriate for the full set of DSCs. The active router shelf controls all the DSCs, while the other router shelf functions purely as a backup. If the active router shelf fails, all DSCs restart under the control of the backup router shelf, which then functions as the active router shelf.

Only one router shelf has control of the DSCs at a time; the other keeps trying to take control but is unable to, and does not interfere with operation of the active router shelf. If, however, the active router shelf crashes, then it relinquishes control of all DSCs to the other router shelf, which restarts the DSCs and commences normal operation. If the crashed router shelf recovers or is restarted, it does not take back control of the DSCs, but instead functions as a backup, and takes control again only if the other router shelf fails.

External interfaces cannot share the same IP address between the two routers shelves, to prevent duplicate IP address errors.

Note Triggers for a failover to occur are those that lead to a hub switchover. The main trigger is loss of the link between the active router shelf (the one with control of the cards) and its DSC *as detected by link monitoring on the DSC*. Any router-shelf failures that do not result in this link going down do not cause failover—for example, the active router's egress interface going down does not trigger failover. Conversely, any temporary loss of the link between the active router and a DSC *does* cause failover, even if the router shelf itself does not crash and connectivity is quickly reestablished—for example, if the BIC cable is knocked out and then quickly replaced. In addition, failover is triggered if a DSC connected to the active router shelf goes down and fails to recover within 90 seconds.

Additional Considerations

System Controller

When a system controller is used with a redundant router shelf, router-shelf failover should look like a single router shelf going down briefly and then recovering. With the current system-controller code, this does not work. The Cisco SC3640 expects only a single router shelf to be configured with any given shelf ID. To get around this, a router in backup mode must be prevented from sending Session Definition Protocol (SDP) packets to the Cisco SC3640. In addition, the SDP packets sent by the router shelves to the Cisco SC3640 currently include a field identifying the MAC address of the sending router. The Cisco SC3640 stores this MAC address and, if it subsequently receives another SDP packet containing the same shelf ID but not the same MAC address, it concludes that multiple routers are configured with the same shelf ID and treats this as an error. This is precisely the situation after a failover, when the backup router shelf starts sending SDP packets with the same shelf ID but different MAC address.

To get around this, you must configure a failover group code—an integer that identifies a redundant pair of router shelves. Each member of the pair must be configured with the same group code. When failover mode is enabled, this group code is sent in place of the router MAC address. These changes are all made to the system-controller code that runs on the router shelf itself, rather than on the Cisco SC3640.

Load Sharing

There is no load sharing between the two routers shelves—no calls can go through the backup router shelf. One disadvantage of this is that you cannot split the load between the routers to reduce the number of calls that are lost when a router crashes. There are, however, also some advantages: with load sharing, you must ensure that each router can support the entire dial shelf, since upon failure of a router shelf the surviving router shelf owns all the dial-shelf resources, and therefore has a sudden change in the amount of traffic it is supporting. If care had not been taken to test under failover conditions, at full load the surviving router shelf might be overwhelmed, and perhaps provide degraded service. With a redundant router shelf instead acting purely as a standby, provided that the backup router shelf is the same model as the active router shelf, the load is unchanged after switchover—so no change is expected to the router-shelf performance.

Having a single router shelf active at a time is simpler, and makes it easier to support failover when dealing with external servers such as signaling controllers for SS7, RPMS server, and system controllers.

Hitless Redundancy

When router-shelf failover occurs, all calls associated with the failed router shelf are lost. To maintain calls through router-shelf failure requires mirroring call state and fast failure detection. This shelf-redundancy feature ensures only that resources (particularly trunk lines) do not remain unusable while the router shelf that was controlling them is down.

Network Management

Minimal Simple Network Management Protocol (SNMP) support is provided—a trap is issued when failover occurs, and SNMP variables indicate whether a router shelf is active or on standby. An existing MIB—CISCO-C8500-REDUNDANCY-MIB—defines a suitable trap for issuing on failover.

Benefits

When an active router shelf in a Cisco AS5800 loses communication with its DSC, a backup router shelf can be invoked to automatically take over DSCs controlled by the lost router shelf. This backup method, called redundancy, is provided on the Cisco AS5800 to prevent a single point of failure, subsequent downtime, and user intervention to resolve unrecoverable hardware faults.

Restrictions

Router Shelves

Two router shelves of the same model and configuration must be available for this feature to operate.

External Servers

Although some of the failover functionality exists in the existing code base, ensure that the various external servers that can run with the Cisco AS5800 still function when redundant router shelves are used. The servers of concern at the moment are RPMS, SS7, and System Controller; the first two are discussed below:

- Resource pool management server (RPMS). For Resource Pool Management (RPM) to work, the resource pool manager server (RPMS) must be configured with the same information for both router shelves.
- Signaling System 7 (SS7). In an SS7 setup, the call signaling comes through an external Cisco SC2200 unit rather than directly from the switch over the trunk line (as for CAS and ISDN). For call signaling to work after failover, both router shelves must be connected to the Cisco SC2200 using the SS7 Redundant Link Manager (RLM) feature, which was intended to provide redundant links between a single router shelf and the signaling controller. RLM links must be configured from both the active and standby router shelves—the change of router shelves will look like a change from one redundant link to another.

Related Features and Technologies

RSC Handover Redundancy

The Router Shelf Controller Handover Redundancy feature that is available on the Cisco AS5850 is similar to Router Shelf Redundancy on the Cisco AS5800.

Related Documents

- *AS5800 Operations, Administration, Maintenance, and Provisioning (OAM&P) Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/58_oamp/index.htm
- *Cisco IOS Dial Technologies Configuration Guide*
  http://www.cisco.com/univercd/cc/cc/td/doc/product/software/ios122/122cgcr/fdial_c/index.htm
- *Cisco IOS Dial Technologies Command Reference*
  http://www.cisco.com/univercd/cc/cc/td/doc/product/software/ios122/122cgcr/fdial_r/index.htm
- *Cisco SS7 Interconnect for Access Servers Solution*
  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das22/index.htm
- *Cisco SS7 Dial Access Solution System Integration*
  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/r1/
- *Cisco SC2200 Signaling Controller documentation*
  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/r2/

Supported Platforms

- Cisco AS5800

Table 47 Cisco IOS Release and Platform Support for this Feature

Platform	12.1(5)XV1	12.2(11)T
Cisco AS5800	X	X

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

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

- CISCO-C8500-REDUNDANCY-MIB

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 configuring the router for shelf redundancy, do the following:

- Ensure that your network is up and running.
- Test each router shelf to verify connectivity.

Configuration Tasks

See the following sections for configuration tasks for the Router-Shelf Redundancy feature. Each task in the list is identified as either required or optional:

- Configuring the Cisco AS5800 for Shelf Redundancy (required)
- Configuring the Shelf Redundancy Feature (required)
- Verifying Shelf Redundancy (required)

Configuring the Cisco AS5800 for Shelf Redundancy

	Command	Purpose
Step 1	`Router(config)#` **`redundancy`**	Enters configuration-redundancy mode.
Step 2	`Router(config-red)#` **`failover group-number`** *`group-code`*	Configures router-shelf failover. **Note** Use the same *group-code* argument for both routers. This code is used when the system controller is used and it identifies the two routers as effectively representing the same set of dial-shelf resources.

Connect to each router shelf in turn and enter these commands. Treat router shelves as if they are connected as a split dial-shelf configuration.

Note This configuration by itself is not enough for successful failover to occur. Because there is no automatic synchronization of configuration between router shelves, you must configure each router shelf separately. Typically the two router shelves, active and backup, must have the same configuration except for the IP address on egress interfaces.

Note Since configuration is error prone, test the backup router shelf's configuration to ensure that errors are not discovered only when the active router shelf fails in a production environment.

Configuring the Shelf Redundancy Feature

	Command	Purpose
Step 1	`Router(config)#` **`redundancy`**	Enters configuration-redundancy mode.
Step 2	`Router(config-red)#` **`failover group-number`** *`group-number`*	Sets the router shelf to failover mode. You must enter this command on both router shelves.

Verifying Shelf Redundancy

Use the **show redundancy** command to verify whether the “Shelf is redundant” string is displayed on a redundancy-enabled access server, as illustrated below:

```
Router# show redundancy
T1 1/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Version info of slot 3:  HW: 256, PLD Rev: 1
  Framer Version: 0x8

Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x02,
 Board Hardware Version 1.0, Item Number 32-0-00,
 Board Revision 00, Serial Number 12059498,
 PLD/ISP Version <unset>,  Manufacture Date 19-Jun-1999.

  Framing is ESF, Line Code is AMI, Clock Source is Line.
  Trunk setting is rbs-zero.
  Data in current interval (619 seconds elapsed):
     380 Line Code Violations, 171 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 137 Line Err Secs, 10 Degraded Mins
     137 Errored Secs, 21 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours)
     203903 Line Code Violations, 27284 Path Code Violations,
     7 Slip Secs, 531 Fr Loss Secs, 18414 Line Err Secs, 1431 Degraded Mins
```

The following example shows output from two router shelves configured as a failover pair. The active router shelf is initially RouterA. The commands **show redundancy history** and **show redundancy** have been issued. The **show redundancy** command shows that failover is enabled and shows the configured group number. The **show redundancy** command also shows that this router shelf is the active one of the pair. Compare this output with that from the backup router shelf (RouterB) further below.

Note When RouterA is reloaded, thereby forcing a failover, new entries are shown on RouterB when a **show redundancy history** command is issued after failover has occurred.

Log from the First Router Shelf (RouterA):

```
RouterA#
RouterA# show redundancy history
DSC Redundancy Status Change History:

010215 18:17 Slot -1 DSC:Failover configured -> ACTIVE role by default.
010215 18:18 Slot -1 DSC:Failover -> BACKUP role.
010215 18:18 Slot 12 DSC:Failover -> ACTIVE role.
010215 18:18 Slot 12 DSC:Hub, becoming active - arb timeout

RouterA#
RouterA# show redundancy
failover mode enabled, failover group = 32

Currently ACTIVE role.

DSC in slot 12:

Hub is in 'active' state.
Clock is in 'active' state.
```

```
No connection to slot 13

RouterA#
RouterA# reload
Proceed with reload? [confirm]

*Feb 15 20:19:11.059:%SYS-5-RELOAD:Reload requested
System Bootstrap, Version 11.1(13)CA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Copyright (c) 1997 by cisco Systems, Inc.
C7200 processor with 131072 Kbytes of main memory

rommon 1 >
```

Log from the Second Router Shelf (RouterB):

```
RouterB#
RouterB# show redundancy
failover mode enabled, failover group = 32

Currently BACKUP role.

No connection to slot 12

DSC in slot 13:

Hub is in 'backup' state.
Clock is in 'backup' state.

RouterB#
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Switching to DSC 13
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Failover:changing to active mode
*Feb 16 03:24:54.931:%DIAL13-3-MSG:
02:32:06:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:24:55.491:%OIR-6-INSCARD:Card inserted in slot 12, interfaces administratively
shut down
*Feb 16 03:24:58.455:%DIAL13-3-MSG:
02:32:09:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:25:04.939:%DIAL13-0-MSG:

RouterB# show redundancy
failover mode enabled, failover group = 32

Currently ACTIVE role.

No connection to slot 12

DSC in slot 13:

Hub is in 'active' state.
Clock is in 'backup' state.


RouterB# show redundancy history
DSC Redundancy Status Change History:

010216 03:09 Slot -1 DSC:Failover configured -> BACKUP role.
010216 03:24 Slot 13 DSC:Failover -> ACTIVE role.
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
RouterB#
*Feb 16 03:26:14.079:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 1 Succeeded
*Feb 16 03:26:14.255:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 3 Succeeded
*Feb 16 03:26:14.979:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 10 Succeeded
```

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.

- **redundancy**
- **failover group-number**
- **show redundancy**

Glossary

DSC—dial-shelf controller.

DSIP—Dial Shelf Interconnection Protocol.

RLM—redundant link manager.

RPM—resource pool management.

RPMS—resource pool manager server.

SDP—Session Definition Protocol.

SNMP—Simple Network Management Protocol.

SS7—Signaling System 7.

Route-Switch-Controller Handover Redundancy on the Cisco AS5850

Feature History

Release	Modification
12.2(2)XB1	This feature was introduced on the Cisco AS5850.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5850 platform.

This document describes the Route-Switch-Controller Handover Redundancy feature on the Cisco AS5850. It includes the following sections:

Feature Overview

Route-Switch-Controller Handover Redundancy on the Cisco AS5850, with its provision of handover-split mode, provides the first phase of high availability to the Cisco AS5850 platform.

If your gateway contains two route-switch-controller (RSC) cards, you can configure your Cisco AS5850 into either of two split modes: classic split or handover split.

Classic-Split Mode

Classic-split (the default) mode maximizes system throughput by splitting slots between two RSCs. Each RSC controls a certain set of slots (slots 0–5 are owned by the RSC in slot 6 and slots 8–13 are owned by the RSC in slot 7), and operates as though slots other than those that it controls contain no cards because those cards are controlled by the other RSC. Configuration on each RSC affects only the slots owned by that RSC. Calls on a failed RSC are lost, but calls on the functioning RSC continue normally. Operating a Cisco AS5850 in classic-split mode is the same as having two Cisco AS5850s, each with a separate set of cards.

Handover-Split Mode

Handover-split mode maximizes system availability by allowing an RSC to automatically take control of the slots, cards, and calls of the other RSC should that other RSC fail. Each RSC is configured identically as appropriate for the full set of cards. During normal operation, both RSCs are active, handling their own slots, cards, and calls just as in classic-split mode. Should an RSC fail, the other RSC takes over control of the failed RSC's slots, goes into extraload state, restarts the failed RSC's cards, and handles newly arrived calls on those cards—although calls on the failed RSC are lost at the moment of failure. The failed RSC, should it recover or be restarted, remains in standby state until you instruct the active RSC to hand back its newly acquired slots to the standby RSC. This is, in effect, split dial shelf with handover capability.

Alternately, to use system resources most efficiently, you can operate with one of the two RSCs initially and intentionally in extraload state. In this configuration, RSCA initially controls all slots in the chassis and RSCB is in standby mode, ready to take over should RSCA fail. This allows you to overcome the limits of normal classic-split mode in which, because only six slots are available per RSC, an optimal combination of trunk and DSP cards is difficult to achieve. For more information on performance loads, see the "Restrictions" section.

Benefits

High Availability

RSC Handover Redundancy for the Cisco AS5850, enabled in handover-split mode, eliminates any single point of failure, subsequent downtime, and required user intervention to resolve unrecoverable hardware faults. This improves service availability and reduces both service-affecting time and service interruption.

Restrictions

RSC Card Requirements

You must have two RSC cards installed in your Cisco AS5850 system chassis.

Performance Load and Possible Trunk-Card and Port-Density Limitations

The number of CT3, T1, or E1 trunk cards that your system can support depends on the split mode in which it is configured to operate. In classic-split mode, an RSC card needs to handle the trunk cards in its own half only. In handover-split mode, an RSC card needs to be able to handle the full load of trunk cards across the entire chassis. In either case, the number of trunk cards allowed should not exceed the performance load of the handling RSC card.

For further information about performance loads, refer to the tables on Cisco AS5850 universal port capacities in the overview chapter of *Cisco AS5850 Universal Gateway Operations, Administration, Maintenance, and Provisioning Guide*, available online at
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/sw_conf/index.htm

Throughput Versus Availability

You must choose between maximal throughput and maximal availability:

- Disabling the handover redundancy by configuring classic-split mode provides maximal throughput, at the expense of availability.
- Enabling handover redundancy by configuring handover-split mode provides maximal availability, at the expense of throughput.

Dropped Calls

Calls on a failed RSC, regardless of mode, are lost at the moment of failure.

Fixed Slot Assignments

Slot assignments are fixed and cannot be changed except by a system in handover-split mode during handover. Slots 0–5 are owned by the RSC in slot 6, and slots 8–13 are owned by the RSC in slot 7.

Related Features and Technologies

Router-Shelf Redundancy

The Router-Shelf Redundancy feature that is available on the Cisco AS5800 is similar to RSC Handover Redundancy on the Cisco AS5850.

Related Documents

- *Cisco AS5850 Operations, Administration, Maintenance, and Provisioning Guide,* chapter on provisioning, available from the Cisco AS5850 Product Documentation website

Supported Platforms

- Cisco AS5850 universal gateway

Table 48 Cisco IOS Release and Platform Support for this Feature

Platform	12.2(2)XB1	12.2(11)T
Cisco AS5850	X	X

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 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

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

None

MIBs

- CISCO-RF-MIB

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

Prerequisites

RSC Cards

Be sure that you have two RSC cards installed in your Cisco AS5850, one in slot 6 and one in slot 7.

Trunk Cards

If you have CT3, T1, or E1 trunk cards in your Cisco AS5850, be sure that you have a supportable number. For more information on performance loads, see the "Restrictions" section on page 776.

Cisco IOS Image

- For classic-split mode, it is advisable, although not mandatory, to configure each RSC with the same Cisco IOS image.

- For handover-split mode, it is mandatory that you configure each RSC with the same Cisco IOS image and the same configuration except for the IP address on egress interfaces. Your Cisco IOS image must support redundancy (Cisco IOS Release 12.2(2)XB, Cisco IOS Release 12.2(11)T, or later releases).

  You must replicate the startup configuration for all line cards in the system in both RSCs' saved configurations to ensure correct operation after a handover.
- You can download software configurations to your Cisco AS5850 using Simple Network Management Protocol (SNMP) or a Telnet connection. To learn how to upgrade your Cisco IOS image, go to the Cisco.com website for Cisco AS5850 Product Documentation, locate the *Cisco AS5850 Universal Gateway Operations, Administration, Maintenance, and Provisioning Guide*, and consult the chapter on provisioning.

Configuration Tasks

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional. Note that you must configure and verify either classic-split mode (the default) or handover-split mode.

- Configuring Classic-Split Mode (optional)
- Verifying Classic-Split Mode (optional)

  or
- Configuring Handover-Split Mode (required)
- Verifying Handover-Split Mode (required)

Configuring Classic-Split Mode

	Command	Purpose
Step 1	`Router#` **`configuration terminal`**	Enters configuration mode.
Step 2	`Router(config)#` **`redundancy`**	Enters configuration-redundancy mode.
Step 3	`Router(config-red)#` **`mode classic-split`**	Selects classic-split (the default) mode.
Step 4	`Router#` **`copy running-config startup-config`**	Copies the running configuration into the startup configuration.
Step 5	`Router#` **`reload`**	Reloads the RSC.

Connect to each RSC in turn and enter these commands.

Note Classic-split mode is the default mode. If you do not perform these steps, your system defaults to this mode.

Note These steps simply configure the system to classic-split mode. You must also configure each of the cards manually.

A classic-split system appears to SNMP management applications as two separate Cisco AS5850s. You must conduct a console session for each RSC (two console sessions) to configure your splits. The system controller manages a classic-split configuration as two separate Cisco AS5850 universal gateways.

Network management systems (NMSs) such as the Cisco Universal Gateway Manager (Cisco UGM) are available that provide a single system view of multiple points of presence (POPs) as they monitor performance and log accounting data. An NMS has a graphical user interface (GUI); runs on a UNIX SPARC station; and includes a database-management system, polling engine, trap management, and map integration.The NMS can be installed at a remote facility so that you can access multiple systems through a console port or Web interface.

In classic-split mode, it is desirable—and, with an NMS, essential—to use four unique IDs, one for each RSC and one for each set of slots. In some cases, however, it is sufficient to use the same ID for the two RSCs.

Verifying Classic-Split Mode

In classic-split mode, most **show** commands (with exceptions noted below) display information for only those slots owned by the RSC; they look and behave as they would if there were no cards in the slots that the RSC does not own. To see **show** command information for a slot, you must connect to the RSC that owns that slot.

Enter any of the following commands, in any order.

- To display information about all slots, regardless of ownership, enter the **show context all** command in EXEC mode.
- To display information about owned slots, enter the **show context** command in EXEC mode without the **all** option.
- To display additional relevant output, including whether an RSC is running in classic-split mode and, if so, which slots it owns, enter the **show chassis** command in EXEC mode.

```
RouterA# show chassis
System is in classic-split mode, RSC in slot 6.
  Slots owned: 0 1 2 3 4 5
  Slots configured: 0 1 2 3 4 5
  Slots owned by other: 8 9 10 11 12 13
Slot    Board     CPU       DRAM          I/O Memory   State          Elapsed
         Type     Util    Total (free)   Total (free)                 Time
 1      UP324    0%/0%  60159040( 51%) 67108864( 73%)  Up             6d01h
 2      UP324    0%/0%  60159040( 56%) 67108864( 73%)  Up             6d01h
 3      UP324    0%/0%  60159040( 56%) 67108864( 73%)  Up             6d01h
 4  CT3_UP216    0%/0%  60159040( 50%) 67108864( 72%)  Up             6d01h
System set for auto boot


RouterB# show chassis
System is in classic-split mode, RSC in slot 7.
  Slots owned: 8 9 10 11 12 13
  Slots configured: 8 9 10 11 12 13
  Slots owned by other: 0 1 2 3 4 5
Slot    Board     CPU       DRAM          I/O Memory   State          Elapsed
         Type     Util    Total (free)   Total (free)                 Time
 9  CT3_UP216    0%/0%  60159040( 65%) 67108864( 72%)  Up             00:21:46
10      UP324    0%/0%  60159040( 62%) 67108864( 73%)  Up             00:21:48
11      UP324    0%/0%  60159040( 62%) 67108864( 73%)  Up             00:21:49
System set for auto boot
```

- To display all configured clock sources, even those from non-owned cards, enter the **show chassis clocks** command in EXEC mode. Only one RSC can provide the master clock, and it may need to have backup clock sources configured from all cards present, regardless of ownership.

```
RouterA# show chassis clocks
Primary Clock:
--------------
Slot 6:
System primary is Slot: 4 Port: 1 of priority 10
TDM Bus Master Clock Generator State = NORMAL

Backup clocks:
Source  Slot  Port  DS3-Port  Priority      Status      State
-------------------------------------------------------------
Trunk   9     1       0         8            Good        Configured
Trunk   4     21      0         498          Good        Default
Trunk   9     21      0         503          Good        Default


Status of trunk clocks:
-----------------------
      Ds3         2 2 2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 1 1
Slot  Port  Type  8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1
4     0     T3    B B B B B B B G G G G G G G G G G G G G G G G G G G G G
9     0     T3    B B B B B B B G G G G G G G G G G G G G G G G G G G G G
```

Configuring Handover-Split Mode

Perform the following steps on both RSCs so that all cards are configured on both RSCs.

	Command	Purpose
Step 1	`Router# configuration terminal`	Enters configuration mode.
Step 2	`Router(config)# redundancy`	Enters redundancy configuration mode.
Step 3	`Router(config-red)# mode handover-split`	Selects handover-split mode.

Connect to each RSC in turn, change the running configuration so that all cards are configured on this RSC, and perform the following steps.

	Command	Purpose
Step 1	`Router# copy running-config startup-config`	Copies the running configuration into the startup configuration.
Step 2	`Router# dir [/all][filesystem:][file-url]`	Displays a list of files on a file system. Use to verifiy that the new image is loaded to system Flash memory or the FTP server.
Step 3	`Router# reload`	Reloads the RSC.

The net result, when you are done, is that all cards are configured on each RSC.

Note These steps simply configure the system to handover-split mode. You must also manually configure each card on both RSCs.

Note By default, a single RSC can handle only up to two CT3 cards. You can release this restriction by using the **no dial-config-guidelines** command. For more information on performance loads, see the "Restrictions" section on page 776.

Verifying Handover-Split Mode

Enter any of the following commands, in any order.

- To indicate whether handover is enabled and whether this RSC is active or standby, enter the **show redundancy states** command in EXEC mode.

```
RouterA# show redundancy states
       my state = 13 -ACTIVE
     peer state = 13 -ACTIVE
           Mode = Duplex
           Unit = Preferred Primary
        Unit ID = 6

  Redundancy Mode = Handover-split: If one RSC fails, the peer RSC will take over the
feature boards
 Maintenance Mode = Disabled
     Manual Swact = Enabled
   Communications = Up

            client count = 3
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 7
           RF debug mask = 0x0
```

- To display logged handover event, enter the **show redundancy history** command in EXEC mode.

```
RouterA# show redundancy history
Redundancy Facility Event Log:
00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:09 client added: Rsc split dshelf client(19) seq=800
00:00:09 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:09 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:09 RF_PROG_INITIALIZATION(100) Rsc split dshelf client(19) op=0 rc=11
00:00:09 RF_PROG_INITIALIZATION(100) RF_LAST_CLIENT(65000) op=0 rc=11
00:00:09 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:11 RF_STATUS_PEER_PRESENCE(400) op=1
00:00:11 RF_STATUS_PEER_PRESENCE(400) Rsc split dshelf client(19) op=1
00:00:11 RF_STATUS_PEER_COMM(401) op=1
00:00:11 RF_STATUS_PEER_COMM(401) Rsc split dshelf client(19) op=1
00:00:11 my state = NEGOTIATION(3) *peer state = UNKNOWN(0)
00:00:15 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=1
00:00:15 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65000) op=1 rc=0
00:00:15 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=1 rc=0
00:00:17 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Rsc split dshelf client(19) op=3
00:00:17 RF_EVENT_GO_STANDBY(512) op=0
00:00:17 *my state = STANDBY COLD(4) peer state = UNKNOWN(0)
00:00:17 RF_PROG_STANDBY_COLD(101) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:17 RF_PROG_STANDBY_COLD(101) Rsc split dshelf client(19) op=0 rc=11
00:00:17 RF_PROG_STANDBY_COLD(101) RF_LAST_CLIENT(65000) op=0 rc=11
00:00:19 my state = STANDBY COLD(4) *peer state = ACTIVE_EXTRALOAD(14)
00:00:51 Configuration parsing complete
```

```
00:00:53 System initialization complete
00:01:11 RF_STATUS_PEER_PRESENCE(400) op=0
00:01:11 RF_STATUS_PEER_PRESENCE(400) Rsc split dshelf client(19) op=0
00:01:11 my state = STANDBY COLD(4) *peer state = DISABLED(1)
00:01:11 Reloading peer (peer presence lost)
00:01:11 *my state = ACTIVE-FAST(9) peer state = DISABLED(1)
00:01:11 RF_STATUS_MAINTENANCE_ENABLE(403) Rsc split dshelf client(19) op=0
00:01:11 RF_PROG_ACTIVE_FAST(200) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_FAST(200) Rsc split dshelf client(19) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_FAST(200) RF_LAST_CLIENT(65000) op=0 rc=11
00:01:11 *my state = ACTIVE-DRAIN(10) peer state = DISABLED(1)
00:01:11 RF_PROG_ACTIVE_DRAIN(201) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_DRAIN(201) Rsc split dshelf client(19) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_DRAIN(201) RF_LAST_CLIENT(65000) op=0 rc=11
00:01:11 *my state = ACTIVE_PRECONFIG(11) peer state = DISABLED(1)
00:01:11 RF_PROG_ACTIVE_PRECONFIG(202) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_PRECONFIG(202) Rsc split dshelf client(19) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_PRECONFIG(202) RF_LAST_CLIENT(65000) op=0 rc=11
00:01:11 *my state = ACTIVE_POSTCONFIG(12) peer state = DISABLED(1)
00:01:11 RF_PROG_ACTIVE_POSTCONFIG(203) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_POSTCONFIG(203) Rsc split dshelf client(19) op=0 rc=11
00:01:11 RF_PROG_ACTIVE_POSTCONFIG(203) RF_LAST_CLIENT(65000) op=0 rc=11
00:01:11 *my state = ACTIVE(13) peer state = DISABLED(1)
00:01:11 RF_PROG_ACTIVE(204) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:11 RF_PROG_ACTIVE(204) Rsc split dshelf client(19) op=0 rc=11
00:01:11 RF_PROG_ACTIVE(204) RF_LAST_CLIENT(65000) op=0 rc=11
00:01:11 RF_STATUS_PEER_COMM(401) op=0
00:01:11 RF_STATUS_PEER_COMM(401) Rsc split dshelf client(19) op=0
00:01:11 Reloading peer (communication down)
00:01:11 RF_EVENT_GO_ACTIVE_EXTRALOAD(513) RF_INTERNAL_MSG(0) op=0
00:01:11 RF_PROG_EXTRALOAD(301) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:11 RF_PROG_EXTRALOAD(301) Rsc split dshelf client(19) op=0 rc=11
00:01:11 RF_PROG_EXTRALOAD(301) RF_LAST_CLIENT(65000) op=0 rc=11
00:01:11 RF_EVENT_GO_ACTIVE_EXTRALOAD(513) RF_INTERNAL_MSG(0) op=0
00:03:02 RF_STATUS_PEER_PRESENCE(400) op=1
00:03:02 RF_STATUS_PEER_PRESENCE(400) Rsc split dshelf client(19) op=1
00:03:02 RF_STATUS_PEER_COMM(401) op=1
00:03:02 RF_STATUS_PEER_COMM(401) Rsc split dshelf client(19) op=1
00:03:02 *my state = ACTIVE_EXTRALOAD(14) *peer state = UNKNOWN(0)
00:03:02 RF_PROG_PLATFORM_SYNC(300) RF_INTERNAL_MSG(0) op=0 rc=11
00:03:02 RF_PROG_PLATFORM_SYNC(300) Rsc split dshelf client(19) op=0 rc=11
00:03:02 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65000) op=0 rc=0
00:03:02 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=1 rc=0
00:03:02 my state = ACTIVE_EXTRALOAD(14) *peer state = NEGOTIATION(3)
00:03:02 RF_EVENT_PEER_PROG_DONE(506) RF_LAST_CLIENT(65000) op=300
00:03:06 my state = ACTIVE_EXTRALOAD(14) *peer state = STANDBY COLD(4)
6d01h RF_EVENT_GO_ACTIVE_HANDBACK(514) RF_INTERNAL_MSG(0) op=0
6d01h RF_PROG_HANDBACK(302) RF_INTERNAL_MSG(0) op=0 rc=11
6d01h RF_PROG_HANDBACK(302) Rsc split dshelf client(19) op=0 rc=0
6d01h RF_EVENT_CLIENT_PROGRESSION(503) Rsc split dshelf client(19) op=1 rc=0
6d01h RF_EVENT_GO_ACTIVE(511) op=0
6d01h Reloading peer (this unit becoming active)
6d01h *my state = ACTIVE-FAST(9) peer state = STANDBY COLD(4)
6d01h RF_STATUS_MAINTENANCE_ENABLE(403) Rsc split dshelf client(19) op=0
6d01h RF_PROG_ACTIVE_FAST(200) RF_INTERNAL_MSG(0) op=0 rc=11
6d01h RF_PROG_ACTIVE_FAST(200) Rsc split dshelf client(19) op=0 rc=11
6d01h RF_PROG_ACTIVE_FAST(200) RF_LAST_CLIENT(65000) op=0 rc=11
6d01h *my state = ACTIVE-DRAIN(10) peer state = STANDBY COLD(4)
6d01h RF_PROG_ACTIVE_DRAIN(201) RF_INTERNAL_MSG(0) op=0 rc=11
6d01h RF_PROG_ACTIVE_DRAIN(201) Rsc split dshelf client(19) op=0 rc=11
6d01h RF_PROG_ACTIVE_DRAIN(201) RF_LAST_CLIENT(65000) op=0 rc=11
6d01h *my state = ACTIVE_PRECONFIG(11) peer state = STANDBY COLD(4)
6d01h RF_PROG_ACTIVE_PRECONFIG(202) RF_INTERNAL_MSG(0) op=0 rc=11
6d01h RF_PROG_ACTIVE_PRECONFIG(202) Rsc split dshelf client(19) op=0 rc=11
```

```
6d01h RF_PROG_ACTIVE_PRECONFIG(202) RF_LAST_CLIENT(65000) op=0 rc=11
6d01h *my state = ACTIVE_POSTCONFIG(12) peer state = STANDBY COLD(4)
6d01h RF_PROG_ACTIVE_POSTCONFIG(203) RF_INTERNAL_MSG(0) op=0 rc=11
6d01h RF_PROG_ACTIVE_POSTCONFIG(203) Rsc split dshelf client(19) op=0 rc=11
6d01h RF_PROG_ACTIVE_POSTCONFIG(203) RF_LAST_CLIENT(65000) op=0 rc=11
6d01h *my state = ACTIVE(13) peer state = STANDBY COLD(4)
6d01h RF_PROG_ACTIVE(204) RF_INTERNAL_MSG(0) op=0 rc=11
6d01h RF_PROG_ACTIVE(204) Rsc split dshelf client(19) op=0 rc=0
6d01h RF_EVENT_CLIENT_PROGRESSION(503) Rsc split dshelf client(19) op=1 rc=0
6d01h my state = ACTIVE(13) *peer state = ACTIVE(13)
6d01h my state = ACTIVE(13) *peer state = UNKNOWN(0)
6d01h Reloading peer (notification timeout)
6d01h my state = ACTIVE(13) *peer state = ACTIVE(13)
6d01h RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Rsc split dshelf client(19) op=1
6d01h RF_EVENT_GO_ACTIVE(511) op=0
6d01h RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Rsc split dshelf client(19) op=3
6d01h RF_EVENT_GO_ACTIVE(511) op=0
```

- To display details of any pending handover, enter the **show redundancy handover** command in EXEC mode.

```
RouterA# show redundancy handover
No handover pending
```

- To display up to 256 relevant debug entries, enter the **show redundancy debug-log** command in EXEC mode.
- To display additional relevant output, enter the **show chassis** command in EXEC mode. In handover-split mode, this command shows the RSC to be configured with all slots of the entire chassis, regardless of whether the RSC owns the slots or not. Slots owned by the peer RSC are shown to be in the ignore state, properly configured and ready to go.

  The following example shows output for two RSCs in normal-load state.

```
RouterA# show chassis
System is in handover-split mode, RSC in slot 6.
  Slots owned: 0 1 2 3 4 5
  Slots configured: 0 1 2 3 4 5 8 9 10 11 12 13
  Slots owned by other: 8 9 10 11 12 13
Slot    Board     CPU       DRAM          I/O Memory   State         Elapsed
         Type     Util    Total (free)   Total (free)                Time
 1      UP324  17%/17%  60159040( 50%) 67108864( 73%)  Up            6d01h
 2      UP324    1%/0%  60159040( 56%) 67108864( 73%)  Up            6d01h
 3      UP324    0%/0%  60159040( 56%) 67108864( 73%)  Up            6d01h
 4  CT3_UP216    1%/0%  60159040( 49%) 67108864( 72%)  Up            6d01h
 9  CT3_UP216           60159040(  0%) 67108864(  0%)  Ignore        00:00:20
10      UP324           60159040(  0%) 67108864(  0%)  Ignore        00:00:19
11      UP324           60159040(  0%) 67108864(  0%)  Ignore        00:00:18
System set for auto boot


RouterB# show chassis
System is in handover-split mode, RSC in slot 7.
  Slots owned: 8 9 10 11 12 13
  Slots configured: 0 1 2 3 4 5 8 9 10 11 12 13
  Slots owned by other: 0 1 2 3 4 5
Slot    Board     CPU       DRAM          I/O Memory   State         Elapsed
         Type     Util    Total (free)   Total (free)                Time
 1      UP324                  0(  0%)        0(  0%)  Ignore        00:00:38
 2      UP324                  0(  0%)        0(  0%)  Ignore        00:00:37
 3      UP324                  0(  0%)        0(  0%)  Ignore        00:00:36
 4  CT3_UP216                  0(  0%)        0(  0%)  Ignore        00:00:35
 9  CT3_UP216    0%/0%  60159040( 65%) 67108864( 72%)  Up            00:23:14
10      UP324    0%/0%  60159040( 62%) 67108864( 73%)  Up            00:23:16
```

```
11      UP324    0%/0%  60159040( 62%) 67108864( 73%)  Up           00:23:17
System set for auto boot
```

The following example shows output for one RSC in extraload state.

```
RouterA# show chassis
System is in handover-split mode, RSC in slot 6.
  Slots owned: 0 1 2 3 4 5 8 9 10 11 12 13
  Slots configured: 0 1 2 3 4 5 8 9 10 11 12 13
  Slots owned by other: none
Slot    Board     CPU       DRAM          I/O Memory   State         Elapsed
         Type     Util    Total (free)   Total (free)               Time
 1      UP324    0%/0%  60159040( 50%) 67108864( 73%)  Up           6d02h
 2      UP324    1%/0%  60159040( 56%) 67108864( 73%)  Up           6d02h
 3      UP324    0%/0%  60159040( 56%) 67108864( 73%)  Up           6d02h
 4  CT3_UP216    6%/5%  60159040( 49%) 67108864( 72%)  Up           6d02h
 9  CT3_UP216    5%/4%  60159040( 56%) 67108864( 72%)  Up           00:10:29
10      UP324  20%/20%  60159040( 56%) 67108864( 73%)  Up           00:10:30
11      UP324    0%/0%  60159040( 56%) 67108864( 73%)  Up           00:10:30
System set for auto boot
```

Troubleshooting Tips

Command	Purpose
`Router#` **`debug redundancy as5850`**	Enables or disables redundancy-related debug options (hardware lines, master RSC, FSM events, mode, RF client). Use to view specific relevant debug options. All debug entries continue to be logged even if you disable an option here, and you can always use the **show redundancy debug-log** command to view them.

Monitoring and Maintaining Handover Redundancy

Command	Purpose

`Router#` **`redundancy handover`**
{**`cancel`** | **`peer-resources`** | **`shelf-resources`**}
[**`busyout-period`** *`mins`*
`at` *`hh:mm day month year`*]
	Specifies or cancels handover of slots between RSCs. Use during Cisco IOS image upgrades and to return control of slots to an RSC that failed but is now back in service. Specify handover of slots belonging either to the peer RSC (**peer-resources**) or to the RSC on which the command is run (**shelf-resources**). Optionally, specify either or both of the following: length of time for which and exact time at which slots should be busied out before handover.
	Note The **shelf-resources** option causes the RSC to reload.

Note You can detect if an RSC is in extraload with control of the entire chassis resources by observing that the master LED for that RSC is on. You can also detect this state by using the **show redundancy states** command.

The following example shows two instances of handover scheduling, verification, cancellation, and verification of cancellation:

```
RouterA# redundancy handover shelf-resources busyout-period 10 at 16:15 5 Sept 2001
Newly entered handover schedule:
Busyout period at 16:15:00 PST Wed Sep 5 2001 for a duration of 10 minute(s)
Handover pending at 16:25:00 PST Wed Sep 5 2001
Clear calls, handover and reload as specified above?[confirm]

RouterA# show redundancy handover
Busyout period at 16:15:00 PST Wed Sep 5 2001 for a duration of 10 minute(s)
Handover pending at 16:25:00 PST Wed Sep 5 2001

RouterA# redundancy handover cancel
Scheduled handover is cancelled

RSC-Slot6# show redundancy handover
No handover pending



RouterA# redundancy handover peer-resources busyout-period 10 at 16:37 5 Sep 2001
Newly entered handover schedule:
Busyout period at 16:37:00 PST Wed Sep 5 2001 for a duration of 10 minute(s)
Handover pending at 16:47:00 PST Wed Sep 5 2001
Clear calls and handover as specified above?[confirm]

RouterA# show redundancy handover
Busyout period at 16:37:00 PST Wed Sep 5 2001 for a duration of 10 minute(s)
Handover pending at 16:47:00 PST Wed Sep 5 2001

RouterA# redundancy handover cancel
Scheduled handover is cancelled

RouterA# show redundancy handover
No handover pending
```

Configuration Examples

The following example shows a startup configuration that supports redundancy. Note, in the sections on resource-pool range and controller numbers, that every card in the chassis is configured.

```
RouterA# show startup-config

version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname RouterA
!
redundancy
 mode handover-split
aaa new-model
!
!
aaa group server tacacs+ redline2
!
aaa group server radius RADIUS-GROUP
```

```
 server 172.22.51.9 auth-port 1645 acct-port 1646
!
aaa authentication login CONSOLE none
aaa authentication login VTY none
aaa authentication ppp default group RADIUS-GROUP
aaa authentication ppp RADIUS-LIST group RADIUS-GROUP
aaa authorization exec CONSOLE none
aaa authorization exec RADIUS-LIST group RADIUS-GROUP
aaa authorization network default group RADIUS-GROUP if-authenticated
aaa authorization network RADIUS-LIST group RADIUS-GROUP if-authenticated
aaa accounting network default start-stop group RADIUS-GROUP
aaa nas port extended
aaa session-id common
enable password xxx
!
username RouterB password 0 xxx
username 54006
username 54006_1 password 0 xxx
username RouterA password 0 xxx
username 54006_d_119 password 0 xxx
!
resource-pool enable
!
resource-pool group resource group1
 range port 1/0 1/323
 range port 4/20 4/30
!
resource-pool group resource group2
 range port 9/0 9/215
 range port 10/0 10/120
!
resource-pool group resource digital_group_6
 range limit 207
!
resource-pool group resource digital_group
 range limit 116
!
resource-pool group resource vpdn_dig
 range limit 92
!
resource-pool profile customer 54006_customer
 limit base-size all
 limit overflow-size 0
 resource group1 speech
 dnis group 54006_dnis
!
resource-pool profile customer 54007_customer
 limit base-size all
 limit overflow-size 0
 resource group2 speech
 dnis group 54007_dnis
!
resource-pool profile customer 54006_customer_sync
 limit base-size all
 limit overflow-size 0
 resource digital_group_6 digital
 dnis group 54006_sync_dnis
!
resource-pool profile customer 54007_sync
 limit base-size all
 limit overflow-size 0
 resource digital_group digital
 dnis group 54007_sync_dnis
!
```

```
resource-pool profile customer 54007_sync_vpdn
 limit base-size all
 limit overflow-size 0
 resource vpdn_dig digital
 dnis group 54007_sync_vpdn_dnis
clock timezone PST -7
dial-tdm-clock  priority 8 trunk-slot 9 ds3-port 0 port 1
dial-tdm-clock  priority 10 trunk-slot 4 ds3-port 0 port 1
spe country t1-default
!
spe link-info poll voice 5
!
ip subnet-zero
ip cef distributed
ip ftp source-interface FastEthernet6/0
ip ftp username root
ip ftp password xxxxx
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol l2f
 source-ip 30.0.0.1
!
chat-script dial "" "ATZ" OK "ATDT\T" TIMEOUT 60 CONNECT
isdn switch-type primary-5ess
!
controller T3 4/0
 framing c-bit
 cablelength 224
 t1 1-28 controller
!
controller T1 4/0:1
 framing esf
 pri-group timeslots 1-24
!
controller T1 4/0:2
 framing esf
 pri-group timeslots 1-24
!
controller T1 4/0:3
 framing esf
 pri-group timeslots 1-24
!
.
.
.
controller T1 4/0:28
 shutdown
 framing esf
 pri-group timeslots 1-24
!
controller T3 9/0
 framing c-bit
 cablelength 224
 t1 1-28 controller
!
controller T1 9/0:1
 framing esf
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
!
controller T1 9/0:2
```

```
 framing esf
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
!
controller T1 9/0:3
 framing esf
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
!
.
.
.
controller T1 9/0:12
 framing esf
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
!
controller T1 9/0:13
 framing esf
 pri-group timeslots 1-24
!
.
.
.
controller T1 9/0:21
 framing esf
 pri-group timeslots 1-24
!
controller T1 9/0:22
 shutdown
 framing esf
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
!
.
.
.
controller T1 9/0:28
 shutdown
 framing esf
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
!
!
!
interface Loopback0
 ip address 111.111.111.11 255.255.255.0
 no ip mroute-cache
!
interface Serial4/0:1:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
!
interface Serial4/0:2:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
!
interface Serial4/0:3:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
```

```
!
.
.
.
interface Serial4/0:10:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
!
interface Serial4/0:11:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
!
interface Serial9/0:21:23
 ip unnumbered Loopback0
 encapsulation ppp
 ip mroute-cache
 dialer rotary-group 1
 dialer-group 1
 isdn switch-type primary-5ess
!
interface Group-Async0
 ip unnumbered Loopback0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 36000 either
 dialer string 6003
 dialer-group 1
 async default routing
 async mode dedicated
 peer default ip address pool KRAMER
 ppp max-bad-auth 3
 ppp authentication chap pap callin RADIUS_LIST
 ppp chap hostname RouterB
 ppp chap password 7 xxxxx
 group-range 9/00 11/323
!
interface Group-Async1
 ip unnumbered Loopback0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 36000 either
 dialer string 6003
 dialer-group 1
 async default routing
 async mode dedicated
 peer default ip address pool KRAMER1
 ppp max-bad-auth 3
 ppp authentication chap pap callin RADIUS_LIST
 ppp chap hostname RouterA
 ppp chap password 7 xxxxx
 group-range 1/00 4/215
!
interface Dialer0
 ip unnumbered Loopback0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 36000 either
 dialer string 6003
 dialer-group 1
 peer default ip address pool KRAMER1_d_m
 no fair-queue
 no cdp enable
 ppp authentication chap pap callin RADIUS_LIST
 ppp chap hostname RouterA
 ppp chap password 7 xxxxx
 ppp multilink
!
interface Dialer1
 ip unnumbered Loopback0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 36000 either
 dialer string 6003
 dialer-group 1
 peer default ip address pool KRAMER_d
 no cdp enable
 ppp max-bad-auth 3
 ppp authentication chap pap callin RADIUS_LIST
 ppp chap hostname RouterB
 ppp chap password 7 xxxxx
!
interface Dialer2
 ip unnumbered Loopback0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 36000 either
 dialer string 6003
 dialer-group 1
 peer default ip address pool KRAMER1_d
 no fair-queue
 no cdp enable
 ppp authentication chap pap callin RADIUS_LIST
 ppp chap hostname RouterA
 ppp chap password 7 xxxxx
!
interface Dialer5
 no ip address
 no cdp enable
!
interface Dialer6
 no ip address
 no cdp enable
!
interface Dialer7
 no ip address
 no cdp enable
!
.
.
.
interface Dialer26
 no ip address
 no cdp enable
!
ip local pool KRAMER1 10.6.1.1 10.6.1.108
ip local pool KRAMER1 10.6.2.1 10.6.2.108
ip local pool KRAMER1 10.6.3.1 10.6.3.60
ip local pool KRAMER 10.7.1.1 10.7.1.108
ip local pool KRAMER 10.7.2.1 10.7.2.108
ip local pool KRAMER 10.7.3.1 10.7.3.60
ip local pool KRAMER1_d 10.6.4.1 10.6.4.115
ip local pool KRAMER_d 10.7.4.1 10.7.4.115
ip local pool KRAMER1_d_m 10.6.4.116 10.6.4.163
ip classless
no ip http server
!
ip radius source-interface FastEthernet6/0
!
dialer dnis group 54006_dnis
 number 1002
 number 1002100212
!
dialer dnis group 54007_dnis
 number 38327
!
dialer dnis group 54006_sync_dnis
 number 6666
 number 6600
 number 6666666666
!
dialer dnis group 54007_sync_dnis
 number 7700
 number 7700000000
!
dialer dnis group 54007_sync_vpdn_dnis
 number 7777
 number 7777777777
!
dialer dnis group 54007_vpdn_dnis
 number 38777
dialer-list 1 protocol ip permit
no cdp run
!
tacacs-server host 152.22.51.64
tacacs-server timeout 30
tacacs-server key cisco
snmp-server community public RW
snmp-server enable traps rf
!
radius-server configure-nas
radius-server host 172.22.51.9 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 3
radius-server attribute nas-port format c
radius-server key lab
call rsvp-sync
!
voice-port 4/0:1:D
!
voice-port 4/0:2:D
!
.
.
.
voice-port 4/0:28:D
!
voice-port 9/0:1:0
!
voice-port 9/0:2:0
!
.
.
.
voice-port 9/0:28:0
!
!
line con 0
```

```
 password xxxxxx
 logging synchronous
line aux 0
 logging synchronous
 modem InOut
 transport input all
line vty 0 4
 password xxx
 transport preferred telnet
 transport input telnet
line 1/00 4/215
 modem InOut
 no modem status-poll
 no modem log rs232
 transport preferred none
 transport input all
 autoselect during-login
 autoselect ppp
line 9/00 9/215
 modem InOut
 no modem status-poll
 no modem log rs232
 transport preferred none
 transport input all
 autoselect during-login
 autoselect ppp
line 10/00 11/323
 modem InOut
 no modem status-poll
 no modem log rs232
 transport preferred none
 transport input all
 autoselect during-login
 autoselect ppp
!
end
```

Command Reference

MULTIPLE COMMANDS IN FEATURE MODULE

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.

New Commands

- **debug redundancy as5850**
- **mode (redundancy)**
- **redundancy handover**
- **show redundancy (5850)**

Modified Commands

- **show chassis**

Glossary

classic-split mode—Mode in which system throughput is maximized because slots are split between two RSCs.

handover—The ability of one part of a system to take over resources that were managed by another part of the system when the latter part fails.

handover-split mode—Mode in which system availability is maximized because an RSC can automatically take control over the slots, cards, and calls of the other RSC, should that other RSC fail.

RSC—route switch controller. The card that provides switch functions, routing, management control, clock control, and egress ports.

service-affecting time—Amount of time during which the system is unable to take new calls or carry the full number of calls.

service interruption—Event during which an in-progress call is dropped, requiring the user to call back.

Route Processor Redundancy Plus (RPR+)

Route Processor Redundancy (RPR) provides an alternative to the High System Availability (HSA) feature. HSA enables a system to reset and use a standby Route Switch Processor (RSP) if the active RSP fails. Using RPR, you can reduce unplanned downtime because RPR enables a quicker switchover between an active and standby RSP if the active RSP experiences a fatal error.

RPR Plus (RPR+) is an enhancement of the RPR feature. RPR+ keeps the Versatile Interface Processors (VIPs) from being reset and reloaded when a switchover occurs between the active and standby RSPs.

Feature History for the Route Processor Redundancy Plus (RPR+) Feature

Release	Modification
12.0(19)ST1	This feature was introduced.
12.0(22)S	This feature was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.3(7)T	This feature was integrated into Cisco IOS Release 12.3(7)T.

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

- Command Reference, page 806
- Glossary, page 807

Prerequisites for Route Processor Redundancy Plus (RPR+)

RPR and RPR+ require a Cisco 7500 series router loaded with two RSP16s, one RSP16 and one RSP8, two RSP8s, or a combination of RSP2s and RSP4s. If you are using the one RSP16 and one RSP8 combination, you must use the same memory—256 MB—in both RSPs because the secondary RSP must be able to support the primary RSP during a failover.

Restrictions for Route Processor Redundancy Plus (RPR+)

- RSP1s do not support RPR or HSA.
- RPR is supported only on routers that support dual RSPs. Only the Cisco 7507 and Cisco 7513 support dual RSPs.
- RPR+ operates only in a system with VIPs as the line cards. Systems with legacy interface processors default to RPR.
- In RPR+ mode, configuration changes done through Simple Network Management Protocol (SNMP) may not be automatically configured on the standby RSP after a switchover occurs.
- RPR+ does not work on routers configured with MPLS.

Information About Route Processor Redundancy Plus (RPR+)

To configure Route Processor Redundancy Plus (RPR+), you should understand the following concepts:

- RPR, page 796
- RPR+, page 797

RPR

Route Processor Redundancy (RPR) provides an alternative to the High System Availability (HSA) feature currently available on Cisco 7500 series routers. HSA enables a system to reset and use a standby Route Switch Processor (RSP) if the active RSP fails.

Using RPR, you can reduce unplanned downtime. RPR enables a quicker switchover between an active and standby RSP if the active RSP experiences a fatal error. When you configure RPR, the standby RSP loads a Cisco IOS image on bootup and initializes itself in standby mode. In the event of a fatal error on the active RSP, the system switches to the standby RSP, which reinitializes itself as the active RSP, reloads all of the line cards, and restarts the system.

RPR+

The RPR+ feature is an enhancement of the RPR feature on Cisco 7500 series routers. RPR+ keeps the VIPs from being reset and reloaded when a switchover occurs between the active and standby RSPs. Because VIPs are not reset and microcode is not reloaded on the VIPs, and the time needed to parse the configuration is eliminated, switchover time is reduced to 30 seconds.

Table 49 describes the average time for a router to switchover to a standby RSP if the active RSP fails.

Table 49 Average Switchover Time Comparison Table

Feature	Time to Immediately Switch a Packet on New RSP After Failover	Expected Overall Time to Have New RSP in New High Availability State After Failover	Notes
HSA	10 minutes	20 minutes	System default.
RPR	5 minutes	15 minutes	VIPs and legacy interface processors (IPs) supported.
RPR+	30 seconds	11 minutes	VIPs supported.[1]

[1] Legacy IPs default to RPR. To allow RPR+ for VIPs when up to two legacy IPs exist in the router, you must configure the **service single-slot-reload-enable** command. If you do not enable the **service single-slot-reload-enable** command or if you have more than two legacy IPs, all the line cards are reloaded.

Note Table 49 shows average switchover times. Recovery time will vary depending on the configuration of the router.

In Table 49 we have noted that RPR+ supports up to two legacy IPs in the router if the **service single-slot-reload-enable** command is configured. By default, the existence of any legacy IPs in the router causes all the line cards to be reloaded during an RPR+ switchover and a message similar to the following to be displayed:

```
%HA-2-MAX_NO_Quiesce: 1 linecard(s) not quiesced exceeds limit of 0, all slots will be
reloaded.
```

If the **service single-slot-reload-enable** command is configured, then the NO_Quiesce limit is set to two, allowing two quiesce failures during an RPR+ switchover. When more than two legacy IPs exist in the router, all the line cards are reloaded during an RPR+ switchover, and a message similar to the following is displayed:

```
%HA-2-MAX_NO_Quiesce: 3 linecard(s) not quiesced exceeds limit of 2, all slots will be
reloaded.
```

How to Configure Route Processor Redundancy Plus (RPR+)

This section contains the following tasks:

- Copying an Image onto Active and Standby RSPs, page 798 (required)
- Setting the Configuration Register Boot Variable, page 799 (optional)
- Configuring RPR+, page 801 (required)
- Verifying RPR+, page 803 (optional)

Copying an Image onto Active and Standby RSPs

Perform this task to use TFTP to copy a high availability Cisco IOS image onto the active and standby RSPs.

Prerequisites

Before copying a file to flash memory, you must ensure that there is enough space available in flash memory. Compare the size of the file that you are copying to the amount of available flash memory shown. If the space available is less than the space required by the file that you will copy, the copy process will not continue and and error message similar to the following will be displayed:

```
%Error copying tftp://image@server/tftpboot/file-location/image-name (Not enough space on
device).
```

SUMMARY STEPS

1. **enable**
2. **copy tftp slot***slot-number***:**
3. **copy tftp slaveslot***slot-number***:**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **copy tftp slot***slot-number***:**

Use this command to copy a high availability Cisco IOS image onto the flash memory card of the active RSP. The **slot***slot-number* keyword and argument specify the flash memory card of the active RSP.

```
Router# copy tftp slot0:

Address or name of remote host []? ip-address
```

Enter the IP address of the TFTP server that contains the new image.

```
Router# 172.18.2.3

Source filename []? image-name
```

Enter the name of the image file that you are copying to the flash memory card.

```
Router# rsp-pv-mz

Destination file name? [image-name1] <Return>
```

Enter the name under which you want the image file to appear at the destination. The destination name is optional. To use the same image name as the source file, press the Enter key.

```
Accessing tftp://ip-address/...
```

Step 3 **copy tftp slaveslot***slot-number***:**

Use this command to copy a high availability Cisco IOS image onto the flash memory card of the standby RSP. The **slaveslot***slot-number* keyword and argument specify the flash memory card of the standby RSP.

```
Router# copy tftp slaveslot0:

Address or name of remote host []? ip-address
```

Enter the IP address of the TFTP server that contains the new image.

```
Router# 172.18.2.3

Source filename []? image-name
```

Enter the name of the image file that you are copying to the flash memory card.

```
Router# rsp-pv-mz

Destination file name? [image-name1] <Return>
```

Enter the name under which you want the image file to appear at the destination. The destination name is optional. To use the same image name as the source file, press the Enter key.

```
Accessing tftp://ip-address/...
```

What to Do Next

If you do not want to modify the software configuration register boot field, proceed to the "Configuring RPR+" section on page 801.

Setting the Configuration Register Boot Variable

Perform this optional task to modify the software configuration register boot field to ensure that the system boots the same image as that specified by the **hw-module slot image** command in the "Configuring RPR+" section on page 801.

SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**
4. **boot system flash slot***slot-number***:**[*image-name*]
5. **config-register** *value*
6. **exit**
7. **reload**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`show version`**
	Example:
	`Router# show version`
		Displays the current configuration register setting at the end of the display.

Step 3	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 4	**boot system flash slot***slot-number***:**[*image-name*] **Example:** `Router(config)# boot system flash slot0:rsp-pv-mz`	Specifies the filename of an image stored in flash memory. • *slot-number***:**—Specifies the active RSP slot where the flash memory card is located. Valid slot numbers are 0 and 1 for the Cisco 7500 series RSP. • *image-name*—Specifies the name of the image. It is recommended that you set the boot variable so that the system boots the same image as that specified by the **hw-module slot** *slot-number* **image** *file-spec* command. See Step 3 of the "Configuring RPR+" section on page 801.
Step 5	**config-register** *value* **Example:** `Router(config)# config-register 0x2102`	Modifies the existing configuration register setting to reflect the way in which you want to load a system image. • Use the *value* argument to specify the configuration register setting. Valid values are in the range from 0x0 to 0xFFFF. • In this example, when a **reload** command is issued, the router automatically boots the image specified in the **boot system flash** *image-name* configuration.

Step 6	**`exit`**
	Example:
	`Router(config)# exit`
		Exits global configuration mode and returns to privileged EXEC mode.

Step 7	**`reload`**
	Example:
	`Router# reload`
		Reboots the router to make your configuration changes take effect.

Examples

The following is sample partial output from the **show version** command; the output displays the current configuration register setting.

```
Router# show version

Cisco IOS Software, C7500 Software (C7500-IPBASE-MZ), Version 12.3(7)T,  RELEASE)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 16-Jan-04 18:03 by engineer

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
.
.
.
Configuration register is 0x2102
```

Configuring RPR+

Perform this task to configure RPR+.

Restrictions

RPR+ operates only in a system with VIPs as the line cards. Systems with legacy IPs default to RPR mode. Up to two legacy IPs can be supported by RPR+ if the **service single-slot-reload-enable** command is configured. For more details, see the "RPR+" section on page 797.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hw-module slot** *slot-number* **image** *file-spec*
4. Repeat Step 3 for the standby RSP.
5. **redundancy**
6. **mode** {**hsa** | **rpr** | **rpr-plus**}
7. **exit**
8. **copy system:running-config nvram:startup-config**
9. **hw-module sec-cpu reset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hw-module slot** *slot-number* **image** *file-spec* **Example:** `Router(config)# hw-module slot 6 image slot0:rsp-pv-mz`	Specifies a high availability Cisco IOS image to run on an active RSP. • Use the *slot-number* argument to specify the RSP slot. • Use the *file-spec* argument to specify the flash memory card to load the image into and the name of the image. • In this example, the active RSP is loaded in slot 6.
Step 4	Repeat Step 3 for the standby RSP. **Example:** `Router(config)# hw-module slot 7 image slot0:rsp-pv-mz`	Repeat Step 3 to specify a high availability Cisco IOS image to run on the standby RSP. • In this example, the standby RSP is loaded in slot 7.
Step 5	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.

Step 6	**mode** {**hsa** | **rpr** | **rpr-plus**}
	Example:
	`Router(config-r)# mode rpr-plus`
		Configures the redundancy mode.
		• Use the **rpr-plus** keyword to configure the mode as RPR+ on both the active and standby RSPs.
		• If no mode is specified, the default mode is HSA.

Step 7	**exit** **Example:** `Router(config-r)# exit`	Exits redundancy configuration mode and returns to global configuration mode. • Repeat this step one more time to exit global configuration mode. • Exiting global configuration mode after the redundancy mode has been set to RPR+ will trigger a timer to run for a few seconds, after which the standby RSP resets and reloads.

	Command or Action	Purpose

Step 8	**`copy system:running-config nvram:startup-config`**
	Example:
	`Router# copy system:running-config nvram:startup-config`
		(Optional) Copies the running configuration to the startup configuration to save the RPR+ configuration.
		• This command can be run manually immediately after exiting global configuration mode when the redundancy mode is set to RPR+, or it can be run after the standby RSP is reloaded and initialized.

Step 9	**`hw-module sec-cpu reset`**
	Example:
	`Router# hw-module sec-cpu reset`
		(Optional) Resets and reloads the standby RSP with the specified Cisco IOS image and executes the image.
		• Although changing the redundancy mode to RPR+ will trigger a reload, using this command may initiate the standby RSP reset a few seconds faster than the automatic reload.
		Note If you do not specify a Cisco IOS image in Step 3, this command loads and executes the bundled default Cisco IOS standby image. The system then operates in HSA mode.

Verifying RPR+

Perform this task to verify whether RPR+ is configured on the router and to display other redundancy statistics.

SUMMARY STEPS

1. **enable**
2. **show redundancy**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show redundancy**

Use this command to verify what type of redundancy is configured on the router and to display other redundancy information.

```
Router# show redundancy

Operating mode is rpr-plus
redundancy mode rpr-plus
hw-module slot 2 image disk0:rsp-pv-mz
hw-module slot 3 image disk0:rsp-pv-mz
```

```
The system total uptime since last reboot is 5 days, 19 hours 36 minutes.
The system has experienced 27 switchovers.
The system has been active (become master) for 5 days, 15 hours 14 minutes.
Reason for last switchover:User forced.
```

Configuration Examples for Route Processor Redundancy Plus (RPR+)

This section contains the following example:

- Configuring RPR+: Example, page 804

Configuring RPR+: Example

In the following example, the active RSP is installed in slot 2 and the standby RSP is installed in slot 3 of a Cisco 7507 router.

```
Router# copy tftp slot0:rsp-pv-mz
Router# copy tftp slaveslot0:rsp-pv-mz
Router# configure terminal
Router(config)# hw-module slot 2 image slot0:rsp-pv-mz
Router(config)# hw-module slot 3 image slot0:rsp-pv-mz
Router(config)# redundancy
Router(config-r)# mode rpr-plus
Router(config-r)# end
Router# hw-module sec-cpu reset
Router# show running-config
version 12.3(7)T
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service single-slot-reload-enable
!
hostname Router
!
boot system rcp://path/to/image/rsp-boot-mz
boot system tftp://path/to/image/rsp-boot-mz
boot bootldr bootflash:rsp-boot-mz
enable password password
!
redundancy
 mode rpr-plus ! Indicates that redundancy mode has been configured for RPR+.
!
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
ip subnet-zero
ip rcmd remote-username Router
ip cef distributed
ip host iphost 192.168.0.1
mpls traffic-eng auto-bw timers
!
!
controller T3 6/0/0
 clock source line
!
!
```

```
interface Ethernet0/0/0
 ip address 10.0.0.1 255.255.0.0
 no ip directed-broadcast
 ip route-cache distributed
 no keepalive
.
.
.
exec-timeout 0 0
 history size 40
 transport preferred none
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Additional References

The following sections provide references related to RPR+.

Related Documents

Related Topic	Document Title
File management and other configuration commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Configuration Fundamentals and Network Management Command Reference*, Release 12.3 T
File management and other configuration examples	*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*
Fast Software Upgrade	*Route Processor Redundancy and Fast Software Upgrade on Cisco 7500 Series Routers* feature document, Release 12.0(16)ST
Single Line Card Reload (SLCR)	*Cisco 7500 Single Line Card Reload* feature document, Release 12.1(5a)E

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

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 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.

- **hw-module sec-cpu reset**
- **hw-module slot image**
- **redundancy**
- **redundancy force-switchover**
- **show redundancy (HSA redundancy)**

Glossary

Active RSP—The RSP that controls and runs the routing protocols and that presents the system management interface.

HSA—High System Availability. HSA enables a system to reset and use a standby RSP if the active RSP fails.

RPR—Route Processor Redundancy. An alternative to HSA that reduces unplanned downtime.

RPR+—Route Processor Redundancy Plus. An enhancement to RPR in which the standby RSP is fully initialized. An RPR+ switchover does not involve resetting line cards or reloading line card software for VIPs. Legacy interface processors are reset and reloaded during switchover.

RSP—Route Switch Processor. The Route Processor on the Cisco 7500 series router.

Standby RSP—The RSP that waits ready to take over the functions of the active RSP in the event of unplanned or planned downtime.

Note Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.