



## **Cisco IOS Command Summary Volume 2 of 3**

Release 12.2

### **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-7811757=  
Text Part Number: 78-11757-01

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.

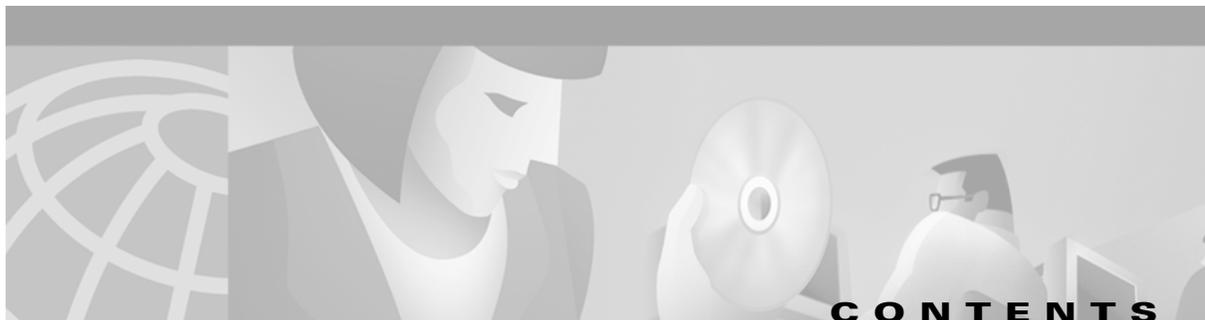
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

*Cisco IOS Command Summary, Volume 2 of 3*  
Copyright © 2001, Cisco Systems, Inc.  
All rights reserved.



**About Cisco IOS Software Documentation**   vii

**Using Cisco IOS Software**   xvii

---

## **Wide-Area Networking**

**ATM Commands**   CS2-3

**Broadband Access: PPP and Routed Bridge Encapsulation Commands**   CS2-51

**Frame Relay Commands**   CS2-57

**Frame Relay-ATM Interworking Commands**   CS2-91

**SMDS Commands**   CS2-95

**X.25 and LAPB Commands**   CS2-101

---

## **Security**

**Authentication Commands**   CS2-139

**Authorization Commands**   CS2-155

**Accounting Commands**   CS2-159

**RADIUS Commands**   CS2-169

**TACACS+ Commands**   CS2-183

**Kerberos Commands**   CS2-187

**Lock-and-Key Commands**   CS2-193

**Reflexive Access List Commands**   CS2-195

**TCP Intercept Commands**   CS2-199

**Context-Based Access Control Commands**   CS2-203

**Cisco IOS Firewall Intrusion Detection System Commands**   CS2-211

**Authentication Proxy Commands**   CS2-219

**Port to Application Mapping Commands CS2-223**

**IPSec Network Security Commands CS2-225**

**Certification Authority Interoperability Commands CS2-235**

**Internet Key Exchange Security Protocol Commands CS2-243**

**Passwords and Privileges Commands CS2-251**

**IP Security Options Commands CS2-259**

**Unicast Reverse Path Forwarding Commands CS2-267**

**Secure Shell Commands CS2-269**

---

## **Interface**

**Interface Commands: aps authenticate Through interface ctunnel CS2-275**

**Interface Commands: interface fastethernet Through service-module t1 remote-loopback CS2-317**

**Interface Commands: service-module t1 timeslots Through yellow CS2-351**

---

## **Dial Technologies**

**Dial Technologies Commands: aaa authorization configuration default Through ds0-group CS2-391**

**Dial Technologies Commands: encapsulation cpp Through modem-pool CS2-445**

**Dial Technologies Commands: multilink bundle-name Through shelf-id CS2-495**

**Dial Technologies Commands: show async status Through show rlm group timer CS2-529**

**Dial Technologies Commands: show sessions Through x25 map ppp CS2-557**

---

## **Terminal Services**

**Terminal Services Commands: absolute-timeout Through show xremote line CS2-591**

**Terminal Services Commands: slip Through xremote xdm CS2-621**

---

**Switching Services**

**Switching Services Commands: access-list rate-limit Through lane fssrp CS2-655**

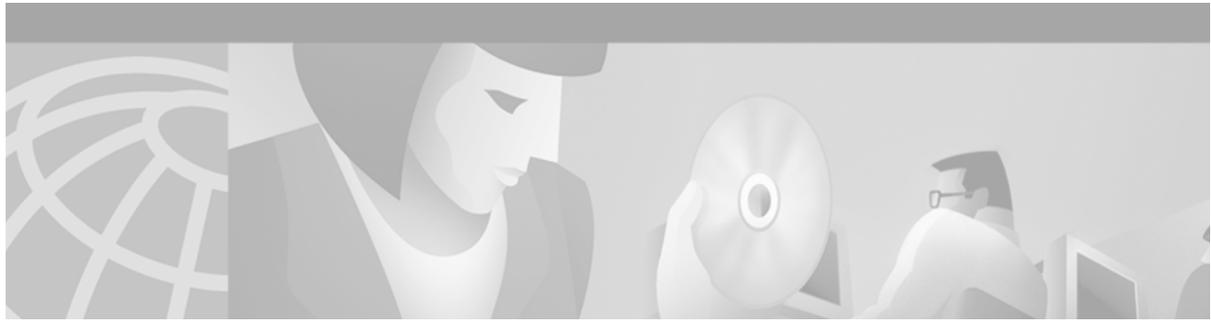
**Switching Services Commands: lane global-lecs-address Through show interface stats CS2-683**

**Switching Services Commands: show interface XTagATM Through tunnel tsp-hop CS2-711**

---

**Index**





# About Cisco IOS Software Documentation

---

This chapter discusses the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation from Cisco Systems.

## Documentation Objectives

Cisco IOS software documentation describes the tasks and commands necessary 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 tasks, the relationship between 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

The Cisco IOS software documentation set consists of documentation modules and master indexes. In addition to the main documentation set, there are supporting documents and resources.

## Documentation Modules

The Cisco IOS documentation modules consist of configuration guides and corresponding command reference publications. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference publication provide complete Cisco IOS command syntax information. Use each configuration guide in conjunction with its corresponding command reference publication.

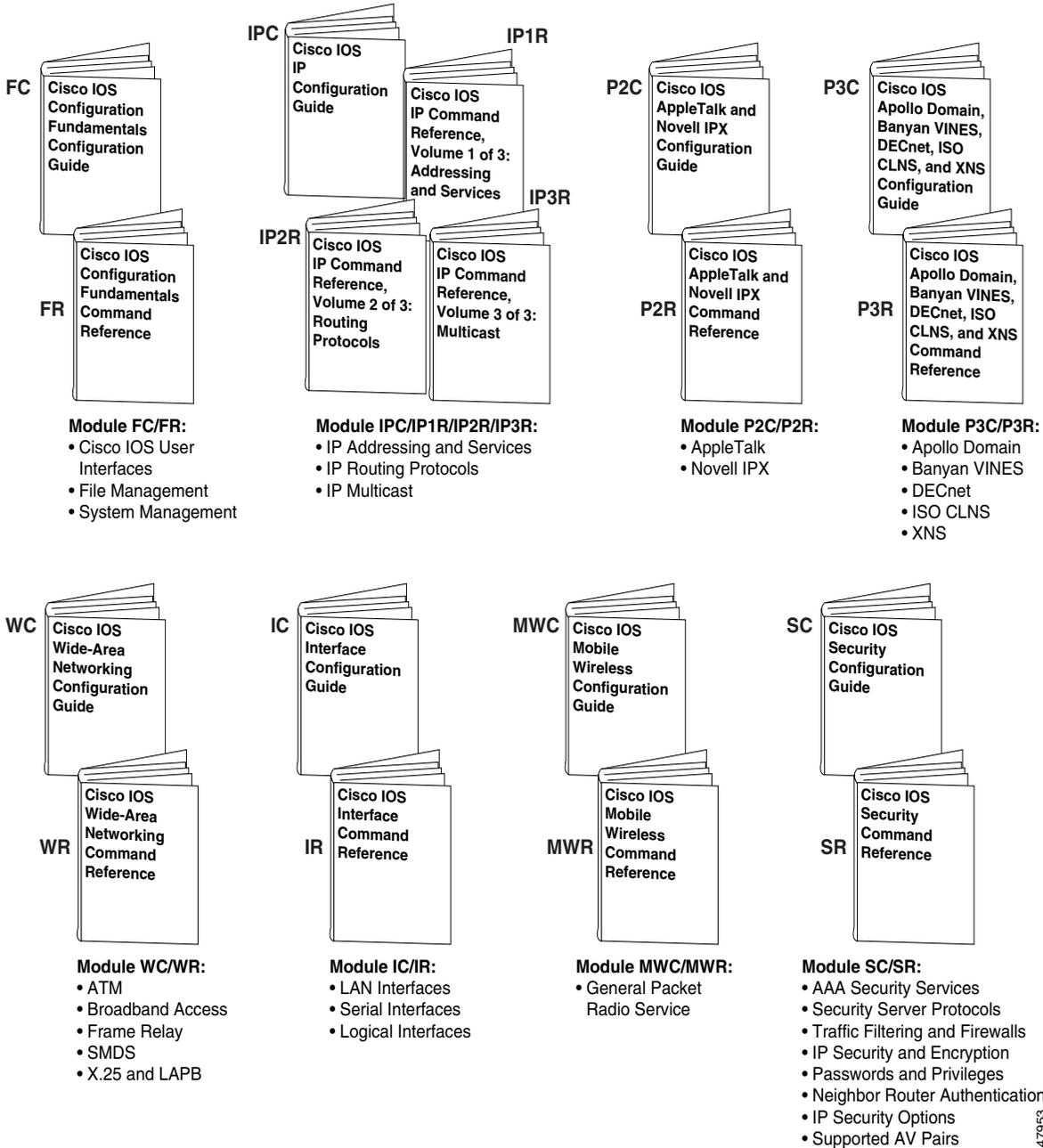
Figure 1 shows the Cisco IOS software documentation modules.



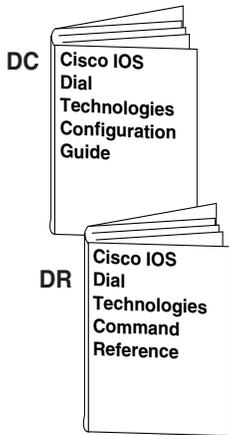
**Note**

The abbreviations (for example, FC and FR) next to the book icons are page designators, which are defined in a key in the index of each document to help you with navigation. The bullets under each module list the major technology areas discussed in the corresponding books.

**Figure 1 Cisco IOS Software Documentation Modules**

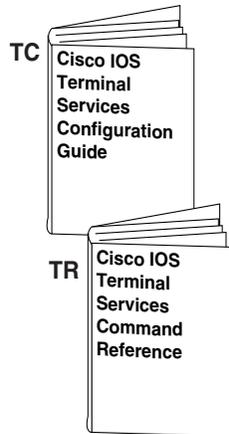


4-7953



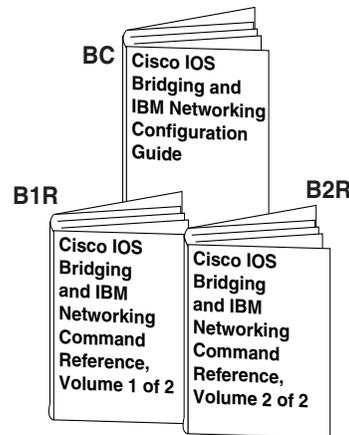
**Module DC/DR:**

- Preparing for Dial Access
- Modem and Dial Shelf Configuration and Management
- ISDN Configuration
- Signalling Configuration
- Dial-on-Demand Routing Configuration
- Dial-Backup Configuration
- Dial-Related Addressing Services
- Virtual Templates, Profiles, and Networks
- PPP Configuration
- Callback and Bandwidth Allocation Configuration
- Dial Access Specialized Features
- Dial Access Scenarios



**Module TC/TR:**

- ARA
- LAT
- NAS1
- Telnet
- TN3270
- XRemote
- X.28 PAD
- Protocol Translation

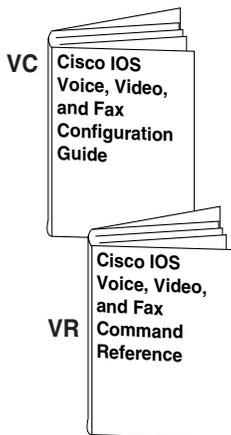


**Module BC/B1R:**

- Transparent Bridging
- SRB
- Token Ring Inter-Switch Link
- Token Ring Route Switch Module
- RSRB
- DLSw+
- Serial Tunnel and Block Serial Tunnel
- LLC2 and SDLC
- IBM Network Media Translation
- SNA Frame Relay Access
- NCIA Client/Server
- Airline Product Set

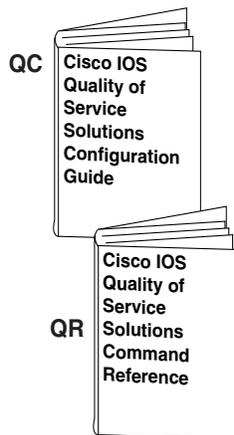
**Module BC/B2R:**

- DSPU and SNA Service Point
- SNA Switching Services
- Cisco Transaction Connection
- Cisco Mainframe Channel Connection
- CLAW and TCP/IP Offload
- CSNA, CMPC, and CMPC+
- TN3270 Server



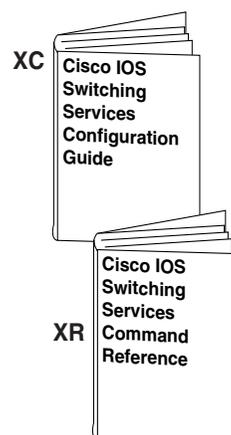
**Module VC/VR:**

- Voice over IP
- Call Control Signalling
- Voice over Frame Relay
- Voice over ATM
- Telephony Applications
- Trunk Management
- Fax, Video, and Modem Support



**Module QC/QR:**

- Packet Classification
- Congestion Management
- Congestion Avoidance
- Policing and Shaping
- Signalling
- Link Efficiency Mechanisms



**Module XC/XR:**

- Cisco IOS Switching Paths
- NetFlow Switching
- Multiprotocol Label Switching
- Multilayer Switching
- Multicast Distributed Switching
- Virtual LANs
- LAN Emulation

47954

## Master Indexes

Two master indexes provide indexing information for the Cisco IOS software documentation set: an index for the configuration guides and an index for the command references. Individual books also contain a book-specific index.

The master indexes provide a quick way for you to find a command when you know the command name but not which module contains the command. When you use the online master indexes, you can click the page number for an index entry and go to that page in the online document.

## Supporting Documents and Resources

The following documents and resources support the Cisco IOS software documentation set:

- *Cisco IOS Command Summary* (three volumes)—This publication explains the function and syntax of the Cisco IOS software commands. For more information about defaults and usage guidelines, refer to the Cisco IOS command reference publications.
- *Cisco IOS System Error Messages*—This publication lists and describes Cisco IOS system error messages. Not all system error 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*—This publication contains an alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, usage guidelines, and sample output.
- *Dictionary of Internetworking Terms and Acronyms*—This Cisco publication compiles and defines the terms and acronyms used in the internetworking industry.
- New feature documentation—The Cisco IOS software documentation set documents the mainline release of Cisco IOS software (for example, Cisco IOS Release 12.2). New software features are introduced in early deployment releases (for example, the Cisco IOS “T” release train for 12.2, 12.2(x)T). Documentation for these new features can be found in standalone documents called “feature modules.” Feature module documentation describes new Cisco IOS software and hardware networking functionality and is available on Cisco.com and the Documentation CD-ROM.
- Release notes—This documentation describes system requirements, provides information about new and changed features, and includes other useful information about specific software releases. See the section “Using Software Release Notes” in the chapter “Using Cisco IOS Software” for more information.
- Caveats documentation—This documentation provides information about Cisco IOS software defects in specific software releases.
- 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 on the World Wide Web at <http://www.rfc-editor.org/>.
- MIBs—MIBs are used for network monitoring. For lists of supported MIBs by platform and release, and to download MIB files, see the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

# New and Changed Information

Since the last release, the *Cisco IOS Command Summary* has been expanded into three volumes.

*Cisco IOS Command Summary, Volume 1 of 3* contains the following sections:

- Configuration Fundamentals
- IP: Addressing and Services
- IP: Routing Protocols
- IP: Multicast
- AppleTalk and Novell IPX
- Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS

*Cisco IOS Command Summary, Volume 2 of 3* contains the following sections:

- Wide-Area Networking
- Security
- Interface
- Dial Technologies
- Terminal Services
- Switching Services

*Cisco IOS Command Summary, Volume 3 of 3* contains the following sections:

- Bridging and IBM Networking, Volume 1 of 2
- Bridging and IBM Networking, Volume 2 of 2
- Quality of Service Solutions
- Voice, Video, and Fax
- Mobile Wireless

## 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.
<i>string</i>	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
<b>boldface</b>	Boldface text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	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.
<b>boldface screen</b>	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.
!	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 helpful suggestions or references to materials not contained in this manual.



#### Timesaver

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

# Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

## World Wide Web

The most current Cisco documentation is available on the World Wide Web at the following website:

<http://www.cisco.com>

Translated documentation is available at the following website:

[http://www.cisco.com/public/countries\\_languages.html](http://www.cisco.com/public/countries_languages.html)

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation can be ordered in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.  
Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

### Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

### Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

## Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.





## Using Cisco IOS Software

---

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

- Understanding Command Modes
- Getting Help
- Using the no and default Forms of Commands
- Saving Configuration Changes
- Filtering Output from the show and more Commands
- Identifying Supported Platforms

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

For information on the conventions used in the Cisco IOS software documentation set, see the chapter “About Cisco IOS Software Documentation” located at the beginning of this book.

## 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 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 the CLI, you are 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, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear 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 <b>logout</b> command.
Privileged EXEC	From user EXEC mode, use the <b>enable</b> EXEC command.	Router#	To return to user EXEC mode, use the <b>disable</b> command.
Global configuration	From privileged EXEC mode, use the <b>configure terminal</b> privileged EXEC command.	Router(config)#	To return to privileged EXEC mode from global configuration mode, use the <b>exit</b> or <b>end</b> command, or press <b>Ctrl-Z</b> .
Interface configuration	From global configuration mode, specify an interface using an <b>interface</b> command.	Router(config-if)#	To return to global configuration mode, use the <b>exit</b> command. To return to privileged EXEC mode, use the <b>end</b> command, or press <b>Ctrl-Z</b> .
ROM monitor	From privileged EXEC mode, use the <b>reload</b> EXEC command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the <b>continue</b> command.

For more information on command modes, refer to the “Using the 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
<b>help</b>	Provides a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
<i>abbreviated-command-entry&lt;Tab&gt;</i>	Completes a partial command name.
<b>?</b>	Lists all commands available for a particular command mode.
<i>command ?</i>	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
<pre>Router&gt; enable Password: &lt;password&gt; Router#</pre>	Enter the <b>enable</b> command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Router#.
<pre>Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	Enter the <b>configure terminal</b> privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.
<pre>Router(config)# interface serial ? &lt;0-6&gt;      Serial interface number Router(config)# interface serial 4 ? / Router(config)# interface serial 4/ ? &lt;0-3&gt;      Serial interface number Router(config)# interface serial 4/0 Router(config-if)#</pre>	<p>Enter interface configuration mode by specifying the serial interface that you want to configure using the <b>interface serial</b> global configuration command.</p> <p>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.</p> <p>You are in interface configuration mode when the prompt changes to Router(config-if)#.</p>

**Table 2** How to Find Command Options (continued)

Command	Comment
<pre>Router(config-if)# ? Interface configuration commands: . . . ip                Interface Internet Protocol config commands keepalive         Enable keepalive lan-name          LAN Name command llc2              LLC2 Interface Subcommands load-interval     Specify interval for load calculation for an                   interface locaddr-priority  Assign a priority group logging           Configure logging for interface loopback         Configure internal loopback on an interface mac-address       Manually set interface MAC address mls               mls router sub/interface commands mpoa             MPOA interface configuration commands mtu              Set the interface Maximum Transmission Unit (MTU) netbios          Use a defined NETBIOS access list or enable                   name-caching no               Negate a command or set its defaults nrzi-encoding     Enable use of NRZI encoding ntp              Configure NTP . . . Router(config-if)#</pre>	<p>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.</p>
<pre>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</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip</b> command.</p> <p>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>

**Table 2** How to Find Command Options (continued)

Command	Comment
<pre>Router(config-if)# ip address ?   A.B.C.D          IP address   negotiated       IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip address</b> command.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you must enter an IP address or the <b>negotiated</b> keyword.</p> <p>A carriage return (&lt;cr&gt;) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>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</pre>	<p>Enter the keyword or argument you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>A &lt;cr&gt; is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?   secondary       Make this IP address a secondary address   &lt;cr&gt; Router(config-if)# ip address 172.16.0.1 255.255.255.0</pre>	<p>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you can enter the <b>secondary</b> keyword, or you can press <b>Enter</b>.</p> <p>A &lt;cr&gt; is displayed; you can press <b>Enter</b> to complete the command, or you can enter another keyword.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>In this example, Enter is pressed to complete the command.</p>

## 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 also can 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 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

In Cisco IOS Release 12.0(1)T and later releases, 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, refer to the “Using the Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

# Identifying Supported Platforms

Cisco IOS software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS software image, see the following sections:

- Using Feature Navigator
- Using Software Release Notes

## Using Feature Navigator

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

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at [cdbadmin@cisco.com](mailto:cdbadmin@cisco.com). If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

## Using Software Release Notes

Cisco IOS software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- Microcode support information
- Feature set tables
- Feature descriptions
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases.





## **Wide-Area Networking**





## ATM Commands

---

This chapter describes the function and syntax of the ATM commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Wide-Area Networking Command Reference*.

### abr

To select available bit rate (ABR) quality of service (QoS) and configure the output peak cell rate and output minimum guaranteed cell rate for an ATM permanent virtual circuit (PVC) or virtual circuit (VC) class, use the **abr** command in the appropriate command mode. To remove the ABR parameters, use the **no** form of this command.

```
abr output-pcr output-mcr
```

```
no abr output-pcr output-mcr
```

---

#### Syntax Description

<i>output-pcr</i>	The output peak cell rate in kilobits per second.
<i>output-mcr</i>	The output minimum guaranteed cell rate in kilobits per second.

---

### atm aal aal3/4

To enable support for ATM adaptation layer 3/4 (AAL3/4) on an ATM interface, use the **atm aal aal3/4** interface configuration command. To disable support for ATM adaptation layer 3/4 (AAL3/4) on an ATM interface, use the **no** form of this command.

```
atm aal aal3/4
```

```
no atm aal aal3/4
```

---

#### Syntax Description

This command has no arguments or keywords.

## atm abr rate-factor

To configure the amount by which the cell transmission rate increases or decreases in response to flow control information from the network or destination for available bit rate (ABR) virtual circuits (VCs), use the **atm abr rate-factor** interface configuration command. To return to the default, use the **no** form of this command.

**atm abr rate-factor** [*rate-increase-factor*] [*rate-decrease-factor*]

**no atm abr rate-factor** [*rate-increase-factor*] [*rate-decrease-factor*]

<b>Syntax Description</b>	<i>rate-increase-factor</i>	(Optional) Factor by which to increase the data rate. The rate increase factor is specified in powers of 2 from 1 to 32768.
	<i>rate-decrease-factor</i>	(Optional) Factor by which to decrease the data rate. The rate decrease factor is specified in powers of 2 from 1 to 32768.

## atm address-registration

To enable the router to engage in address registration and callback functions with the Interim Local Management Interface (ILMI), use the **atm address-registration** interface configuration command. To disable ILMI address registration functions, use the **no** form of this command.

**atm address-registration**

**no atm address-registration**

**Syntax Description** This command has no arguments or keywords.

## atm arp-server

To identify an ATM Address Resolution Protocol (ARP) server for the IP network or set time-to-live (TTL) values for entries in the ATM ARP table, use the **atm arp-server** interface configuration command. To remove the definition of an ATM ARP server, use the **no** form of this command.

**atm arp-server** [**self** [**time-out** *minutes*]] | [**nsap** *nsap-address*]

**no atm arp-server** [**self** [**time-out** *minutes*]] | [**nsap** *nsap-address*]

<b>Syntax Description</b>	<b>self</b>	(Optional) Specifies the current router as the ATM ARP server.
	<b>time-out</b> <i>minutes</i>	(Optional) Number of minutes for which a destination entry listed in the ATM ARP server's ARP table will be kept before the server takes any action to verify or time out the entry.
	<b>nsap</b> <i>nsap-address</i>	(Optional) Network service access point (NSAP) address of an ATM ARP server.

## atm clock internal

To cause the ATM interface to generate the transmit clock internally, use the **atm clock internal** interface configuration command. To restore the default value, use the **no** form of this command.

**atm clock internal**

**no atm clock internal**

---

**Syntax Description** This command has no arguments or keywords.

## atm ds3-scramble

To enable scrambling of the ATM cell payload for the DS3 physical layer interface module (PLIM) on an ATM interface, use the **atm ds3-scramble** interface configuration command. To disable scrambling of the ATM cell payload for the DS3 PLIM, use the **no** form of this command.

**atm ds3-scramble**

**no atm ds3-scramble**

---

**Syntax Description** This command has no arguments or keywords.

## atm e164 auto-conversion

To enable ATM E164 autoconversion, use the **atm e164 auto-conversion** interface configuration command. To disable autoconversion, use the **no** form of this command.

**atm e164 auto-conversion**

**no atm e164 auto-conversion**

---

**Syntax Description** This command has no arguments or keywords.

## atm e3-scramble

To enable scrambling of the ATM cell payload for the E3 physical layer interface module (PLIM) on an ATM interface, use the **atm e3-scramble** interface configuration command. To disable scrambling of the ATM cell payload for the E3 PLIM, use the **no** form of this command.

**atm e3-scramble**

**no atm e3-scramble**

---

**Syntax Description** This command has no arguments or keywords.

## atm esi-address

To enter the end station ID (ESI) and selector byte fields of the ATM network service access point (NSAP) address, use the **atm esi-address** interface configuration command. The NSAP address prefix is filled in via Integrated Local Management Interface (ILMI) from the ATM switch. To delete the end station address, use the **no** form of this command.

**atm esi-address** *esi.selector*

**no atm esi-address** *esi.selector*

---

<b>Syntax Description</b>	<i>esi</i>	End station ID field value in hexadecimal; 6 bytes long.
	<i>.selector</i>	Selector field value in hexadecimal; 1 byte long.

---

## atm exception-queue

To set the exception queue length, use the **atm exception-queue** interface configuration command. To restore the default value, use the **no** form of this command.

**atm exception-queue** *number*

**no atm exception-queue**

---

<b>Syntax Description</b>	<i>number</i>	Number of entries, in the range from 8 to 256.
---------------------------	---------------	--

---

## atm framing (DS3)

To specify DS3 line framing on an ATM interface, use the **atm framing** interface configuration command. To return to the default C-bit with Physical Layer Convergence Protocol (PLCP) framing, use the **no** form of this command.

```
atm framing [cbitadm | cbitplcp | m23adm | m23plcp]
```

```
no atm framing [cbitadm | cbitplcp | m23adm | m23plcp]
```

Syntax Description	
<b>cbitadm</b>	(Optional) Specifies C-bit with ATM direct mapping (ADM).
<b>cbitplcp</b>	(Optional) Specifies C-bit with PLCP framing.
<b>m23adm</b>	(Optional) Specifies M23 ATM direct mapping.
<b>m23plcp</b>	(Optional) Specifies M23 with PLCP framing.

## atm framing (E3)

To specify E3 line framing, use the **atm framing** interface configuration command. To return to the default G.751 Physical Layer Convergence Protocol (PLCP) framing, use the **no** form of this command.

```
atm framing [g751adm | g832adm | g751plcp]
```

```
no atm framing [g751adm | g832adm | g751plcp]
```

Syntax Description	
<b>g751adm</b>	(Optional) Specifies G.751 ATM Direct Mapping (ADM).
<b>g832adm</b>	(Optional) Specifies G.832 ATM Direct Mapping.
<b>g751plcp</b>	(Optional) Specifies G.751 PLCP encapsulation.

## atm ilmi-keepalive

To enable Interim Local Management Interface (ILMI) keepalives, use the **atm ilmi-keepalive** interface configuration command. To disable ILMI keepalives, use the **no** form of this command.

```
atm ilmi-keepalive [seconds]
```

```
no atm ilmi-keepalive [seconds]
```

Syntax Description	
<b>seconds</b>	(Optional) Number of seconds between keepalives. Values less than 3 seconds are rounded up to 3 seconds, and there is no upper limit.

## atm ilmi-pvc-discovery

To enable ATM permanent virtual circuit (PVC) discovery, use the **atm ilmi-pvc-discovery** interface configuration command. To disable PVC Discovery, use the **no** form of this command.

**atm ilmi-pvc-discovery** [subinterface]

**no atm ilmi-pvc-discovery** [subinterface]

---

### Syntax Description

**subinterface** (Optional) Causes discovered PVCs to be assigned to the ATM subinterface whose number matches the discovered PVC's VPI number.

---

## atm lbo

To specify the cable length (line build-out) for the ATM interface, use the **atm lbo** interface configuration command. To return to the default, use the **no** form of this command.

**atm lbo** {long | short}

**no atm lbo**

---

### Syntax Description

**long** Specifies a cable length greater than 50 feet.

**short** Specifies a cable length less than 50 feet.

---

## atm max-channels

To configure the number of transmit channels for the interface, use the **atm max-channels** interface configuration command. To return to the default, use the **no** form of this command.

**atm max-channels** *number*

**no atm max-channels**

---

### Syntax Description

*number* Maximum number of transmit channels for the interface. The range is 64 to 2048 channels. The default is 64 channels.

---

## atm maxvc

To set the ceiling value of the virtual circuit descriptor (VCD) on the ATM interface, use the **atm maxvc** interface configuration command. To restore the default value, use the **no** form of this command.

**atm maxvc** *number*

**no atm maxvc**

---

<b>Syntax Description</b>	<i>number</i> Maximum number of supported virtual circuits. Valid values are 256, 512, 1024, or 2048.
---------------------------	---

---

## atm mid-per-vc

To limit the number of message identifier (MID) numbers allowed on each virtual circuit, use the **atm mid-per-vc** interface configuration command.

**atm mid-per-vc** *maximum*

---

<b>Syntax Description</b>	<i>maximum</i> Number of MIDs allowed per virtual circuit on this interface. The values allowed are 16, 32, 64, 128, 256, 512, and 1024.
---------------------------	--

---

## atm multicast

To assign a Switched Multimegabit Data Service (SMDS) E.164 multicast address to the ATM subinterface that supports ATM adaptation layer 3/4 (AAL3/4) and SMDS encapsulation, use the **atm multicast** interface configuration command.

**atm multicast** *address*

---

<b>Syntax Description</b>	<i>address</i> Multicast E.164 address assigned to the subinterface.
---------------------------	--

---

## atm multipoint-interval

To specify how often new destinations can be added to multipoint calls to an ATM switch in the network, use the **atm multipoint-interval** interface configuration command. To return to the default interval, use the **no** form of this command.

**atm multipoint-interval** *interval*

**no atm multipoint-interval** *interval*

---

<b>Syntax Description</b>	<i>interval</i> Interval length in seconds, in the range from 0 to 4294967.
---------------------------	---

---

## atm multipoint-signalling

To enable point-to-multipoint signalling to the ATM switch, use the **atm multipoint-signalling** interface configuration command. To disable point-to-multipoint signalling to the ATM switch, use the **no** form of this command.

**atm multipoint-signalling**

**no atm multipoint-signalling**

---

**Syntax Description** This command has no arguments or keywords.

## atm nsap-address

To set the network service access point (NSAP) address for an ATM interface using switched virtual circuit (SVC) mode, use the **atm nsap-address** interface configuration command. To remove any configured address for the interface, use the **no** form of this command.

**atm nsap-address** *nsap-address*

**no atm nsap-address**

---

**Syntax Description** *nsap-address* The 40-digit hexadecimal NSAP address of this interface (the source address).

---

## atm oam flush

To drop all current and future Operation, Administration, and Maintenance (OAM) cells received on an ATM interface, use the **atm oam flush** interface configuration command. To receive OAM cells on an ATM interface, use the **no** form of this command.

**atm oam flush**

**no atm oam flush**

---

**Syntax Description** This command has no arguments or keywords.

## atm oversubscribe

To manage bandwidth for service categories other than constant bit rate (CBR), use the **atm oversubscribe** global configuration command on a per-ATM-interface basis. To disable bandwidth management, use the **no** form of the command.

**atm oversubscribe**

**no atm oversubscribe**

### Syntax Description

This command has no arguments or keywords.

## atm pvp

To create a permanent virtual path (PVP) used to multiplex (or bundle) one or more virtual circuits (VCs), use the **atm pvp** interface configuration command. To remove a PVP, use the **no** form of this command.

**atm pvp** *vpi* [*peak-rate*]

**no atm pvp** *vpi*

### Syntax Description

<i>vpi</i>	ATM network virtual path identifier (VPI) of the VC to multiplex on the permanent virtual path. The range is 0 to 255. The VPI is an 8-bit field in the header of the ATM cell. The VPI value is unique only on a single link, not throughout the ATM network because it has local significance only. The VPI value must match that of the switch.  The number specified for the <i>vpi</i> must not already exist. If the number specified for the <i>vpi</i> is already being used by an existing VC, this command is rejected.
<i>peak-rate</i>	(Optional) Maximum rate in kbps at which the PVP can transmit data. The range is 84 kbps to line rate. The default is the line rate.

## atm rate-queue

To create a permanent rate queue or specify a rate queue tolerance, use the **atm rate-queue** interface configuration command. To remove a rate queue or rate queue tolerance, use the **no** form of this command.

**atm rate-queue** {*queue-number speed* | **tolerance svc** [*pvc*] *tolerance-value* [**strict**]}

**no atm rate-queue** {*queue-number speed* | **tolerance svc** [*pvc*] *tolerance-value* [**strict**]}

**Syntax Description**

<i>queue-number</i>	Queue number in the range 0 through 7 on the ATM Interface Processor (AIP) for Cisco 7500 series routers, and in the range 0 through 3 on the network processing module (NPM) for Cisco 4500 and Cisco 4700 routers.  On the AIP, queues 0 through 3 are in the high-priority bank, and queues 4 through 7 are in the low-priority bank. Queues in the same priority bank have the same priority; for example, queues 0 and 3 have the same priority. On the NPM, all 4 queues have the same priority.
<i>speed</i>	Speed in megabits per second (Mbps) in the range from 1 through 155. The maximum speed is determined by the detected physical layer interface module (PLIM) type on the AIP or NPM: <ul style="list-style-type: none"> <li>• 34 Mbps for E3</li> <li>• 45 Mbps for DS-3</li> <li>• 100 Mbps for Transparent Asynchronous Transmitter/Receiver Interface (TAXI)</li> <li>• 155 Mbps for Synchronous Optical Network (SONET)</li> </ul>
<b>tolerance</b>	Specifies that you want to use a rate queue tolerance value.
<b>svc</b>	Specifies that the <i>tolerance-value</i> will be applied to SVCs.
<b>pvc</b>	(Optional) If specified, the <i>tolerance-value</i> will be applied to PVCs.
<i>tolerance-value</i>	A tolerance level expressed as a percentage used for assigning rate queues for each virtual circuit (VC) with a requested peak rate. This value is applied to switched virtual circuits (SVCs), discovered VCs, and permanent virtual circuits (PVCs) (when the <b>pvc</b> keyword is used). This value can be 0 or 5 through 99. For SVCs and discovered VCs, the default value is 10. For PVCs, the default value is 0.
<b>strict</b>	(Optional) Indicates whether SVC traffic-shaping parameters are altered beyond the SVC tolerance or rejects the incoming call.

## atm rawq-size

To define the ATM Interface Processor (AIP) raw-queue size, use the **atm rawq-size** interface configuration command. To restore the default value, use the **no** form of this command.

**atm rawq-size** *number*

**no atm rawq-size**

**Syntax Description**

<i>number</i>	Maximum number of cells in the raw queue simultaneously, in the range from 8 through 256.
---------------	---

## atm rxbuff

To set the maximum number of receive buffers for simultaneous packet reassembly, use the **atm rxbuff** interface configuration command. To restore the default value, use the **no** form of this command.

**atm rxbuff** *number*

**no atm rxbuff**

Syntax Description	
<i>number</i>	Maximum number of packet reassemblies that the ATM Interface Processor (AIP) can perform simultaneously, from 0 to 512.

## atmsig close atm

To disconnect a switched virtual circuit (SVC), use the **atmsig close atm EXEC** command.

**AIP on Cisco 7500 series; ATM, ATM-CES, enhanced ATM port adapter on Cisco 7200 series; 1-port ATM-25 network module on Cisco 2600 and 3600 series**

**atmsig close atm** *slot/0 vcd*

**ATM and enhanced ATM port adapter on Cisco 7500 series**

**atmsig close atm** *slot/port-adapter/0 vcd*

**NPM on Cisco 4500 and Cisco 4700**

**atmsig close atm** *number vcd*

Syntax Description	
<i>slot</i>	ATM slot number. Use this format for the following platform configurations: <ul style="list-style-type: none"> <li>AIP on Cisco 7500 series routers.</li> <li>ATM port adapter, ATM-CES port adapter, or enhanced ATM port adapter on Cisco 7200 series routers.</li> <li>1-port ATM-25 network module on Cisco 2600 and 3600 series routers.</li> </ul>
<i>/0</i>	ATM port number. Because the AIP and all ATM port adapters have a single ATM interface, the port number is always 0.
<i>vcd</i>	Virtual circuit descriptor of the signalling SVC to close.
<i>slot/port-adapter</i>	ATM slot number and port adapter number. Use this format for the ATM port adapter or ATM-CES port adapter on Cisco 7500 series routers.
<i>number</i>	ATM network processor module number for the NPM on Cisco 4500 and Cisco 4700 routers.

## atm sig-traffic-shaping strict

To specify that a switched virtual circuit (SVC) should be established on an ATM interface only if shaping can be done per the signaled traffic parameters, use the **atm sig-traffic-shaping strict** interface configuration command. To disable strict traffic shaping, use the **no** form of this command.

```
atm sig-traffic-shaping strict
```

```
no atm sig-traffic-shaping strict
```

---

**Syntax Description** This command has no arguments or keywords.

## atm smds-address

To assign a unicast E.164 address to the ATM subinterface that supports ATM adaptation layer 3/4 (AAL3/4) and Switched Multimegabit Data Service (SMDS) encapsulation, use the **atm smds-address** interface configuration command.

```
atm smds-address address
```

---

**Syntax Description** *address* Unicast E.164 address assigned to the subinterface.

---

## atm sonet stm-1

To set the mode of operation and thus control type of ATM cell used for cell-rate decoupling on the SONET physical layer interface module (PLIM), use the **atm sonet stm-1** interface configuration command. To restore the default Synchronous Transport Signal level 3, concatenated (STS-3c) operation, use the **no** form of this command.

```
atm sonet stm-1
```

```
no atm sonet stm-1
```

---

**Syntax Description** This command has no arguments or keywords.

## atm txbuff

To set the maximum number of transmit buffers for simultaneous packet fragmentation, use the **atm txbuff** interface configuration command. To restore the default value, use the **no** form of this command.

**atm txbuff** *number*

**no atm txbuff**

<b>Syntax Description</b>	<i>number</i>	Maximum number of packet fragmentations that the ATM Interface Processor (AIP) can perform simultaneously, from 0 to 512.
---------------------------	---------------	---

## atm uni-version

To specify the User-Network Interface (UNI) version (3.0 or 3.1) the router should use when Interim Local Management Interface (ILMI) link autodetermination is unsuccessful or ILMI is disabled, use the **atm uni-version** interface configuration command. To restore the default value to 3.0, use the **no** form of this command.

**atm uni-version** *version-number*

**no atm uni-version** *version-number*

<b>Syntax Description</b>	<i>version-number</i>	UNI version selected on an interface. Valid values are 3.0 and 3.1.
---------------------------	-----------------------	---

## atm vc-per-vp

To set the maximum number of virtual channel identifier (VCIs) to support per virtual path identifier (VPI), use the **atm vc-per-vp** interface configuration command. To restore the default value, use the **no** form of this command.

**atm vc-per-vp** *number*

**no atm vc-per-vp**

<b>Syntax Description</b>	<i>number</i>	Maximum number of VCIs to support per VPI. On the AIP for Cisco 7500 series routers, valid values are 16, 32, 64, 128, 256, 512, and 1024.  On the ATM port adapter for Cisco 7200 series and Cisco 7500 series routers, valid values are 16, 32, 64, 128, 256, 512, 1024, and 2048.  On the NPM for Cisco 4500 and Cisco 4700 routers, valid values are 32, 64, 128, 256, 512, 1024, 2048, 4096, and 8192.
---------------------------	---------------	---

## atm vp-filter

To set the ATM Interface Processor (AIP) filter register, use the **atm vp-filter** interface configuration command. To restore the default value, use the **no** form of this command.

**atm vp-filter** *hexvalue*

**no atm vp-filter**

<b>Syntax Description</b>	<i>hexvalue</i>	Value in hexadecimal format.
---------------------------	-----------------	------------------------------

## broadcast

To configure broadcast packet duplication and transmission for an ATM virtual circuit (VC) class, permanent virtual circuit (PVC), switched virtual circuit (SVC), or VC bundle, use the **broadcast** command in the appropriate command mode. To disable transmission of broadcast packets for your ATM VC class, PVC, SVC, or VC bundle, use the **no** form of this command. To restore the default behavior, use the **default** form of this command.

**broadcast**

**no broadcast**

**default broadcast**

<b>Syntax Description</b>	This command has no arguments or keywords.	
---------------------------	--	--

## cbr

To configure the constant bit rate (CBR) for the ATM circuit emulation service (CES) for an ATM permanent virtual circuit (PVC) on the Cisco MC3810, use the **cbr** command in the appropriate configuration mode. To restore the default, use the **no** form of this command.

**cbr** *rate*

**no cbr** *rate*

<b>Syntax Description</b>	<i>rate</i>	Constant bit rate (also known as the average cell rate) for ATM CES. The valid range for this command is from 56 to 10,000 kbps.
---------------------------	-------------	--

## ces

To configure Circuit Emulation Service (CES) on a router port and enter CES configuration mode, use the **ces** global configuration command.

```
ces slot/port
```

<b>Syntax Description</b>	<i>slot/port</i>	Backplane slot number and port number on the interface. The port value is always 0 as the interface configuration applies to all ports in the slot.
---------------------------	------------------	---

## ces aal1 clock

To configure the ATM adaptation layer 1 (AAL1) timing recovery clock for the constant bit rate (CBR) interface, use the **ces aal1 clock** interface configuration command. To return the clock to the default, use the **no** form of this command.

```
ces aal1 clock {adaptive | srts | synchronous}
```

```
no ces aal1 clock
```

<b>Syntax Description</b>	<b>adaptive</b>	Adjusts output clock on a received AAL1 on FIFO basis. Use in unstructured mode.
	<b>srts</b>	Sets the clocking mode to synchronous residual time stamp.
	<b>synchronous</b>	Configures the timing recovery to synchronous for structured mode.

## ces aal1 service

To configure the type of circuit emulation service used on the constant bit rate (CBR) interface, use the **ces aal1 service** interface configuration command. To return the type of service to unstructured, use the **no** form of this command.

```
ces aal1 service {structured | unstructured}
```

```
no ces aal1 service
```

<b>Syntax Description</b>	<b>structured</b>	Sets the type of service to structured (cross-connect).
	<b>unstructured</b>	Sets the type of service to unstructured (clear-channel).

## ces-cdv

To set the cell delay variation, use the **ces-cdv** interface-ATM-VC configuration command.

```
ces-cdv time
```

### Syntax Description

<i>time</i>	Maximum tolerable cell arrival jitter with a range of 1 to 65535 microseconds.
-------------	--

## ces circuit

To configure the connection attributes for the constant bit rate (CBR) interface, use the **ces circuit** interface configuration command. To return the connection attributes to the default or to enable the circuit, use the **no** form of this command.

```
ces circuit circuit-number [cas] [cdv range] [circuit-name name] [on-hook-detection
hex-number] [partial-fill range] [shutdown] [timeslots range]
```

```
no ces circuit circuit-number [cas] [cdv range] [circuit-name name] [on-hook-detection
hex-number] [partial-fill range] [shutdown] [timeslots range]
```

### Syntax Description

<i>circuit-number</i>	Selects the circuit identification. For unstructured service, use 0. For T1 structured service, the range is 1 through 24. For E1 structure service, the range is 1 through 31.
<b>cas</b>	(Optional) Enables channel-associated signalling for structured service only. The default is <b>no cas</b> .
<b>cdv range</b>	(Optional) Enables the peak-to-peak cell delay variation requirement. The range for CDV is 1 through 65535 milliseconds. The default is 2000 milliseconds.
<b>circuit-name name</b>	(Optional) Sets the ASCII name for the circuit emulation service internetworking function CES-IWF circuit. The string for the circuit name is 0 through 255. The default is CBRx/x:0.
<b>on-hook-detection hex-number</b>	(Optional) Enables detection of whether the circuit is on-hook. Hex values are 0 through F to indicate a 2- or 4-bit AB[CD] pattern to detect on-hook. The AB[CD] bits are determined by the manufacturer of the voice/video telephony device that is generating the CBR traffic.
<b>partial-fill range</b>	(Optional) Enables the partial AAL1 cell fill service for structured service only. The range is 0 through 47. The default is 47.
<b>shutdown</b>	(Optional) Marks the CES-IWF circuit administratively down. The default is <b>no shutdown</b> .
<b>timeslots range</b>	(Optional) Configures the time slots for the CES-IWF circuit for structured service only. The range is 1 through 24 for T1. The range is 1 through 31 for E1.

## ces dsx1 clock source

To configure a transmit clock source for the constant bit rate (CBR) interface, use the **ces dsx1 clock source** interface configuration command. To return the clock source to the default, use the **no** form of this command.

```
ces dsx1 clock source {loop-timed | network-derived}
```

```
no ces dsx1 clock source
```

Syntax Description	loop-timed	network-derived
	Configures the transmit clock to loop (RX-clock to TX-clock).	Configures the transmit clock to be derived from the network.

## ces dsx1 framing

To select the frame type for the data line on the constant bit rate (CBR) interface, use the **ces dsx1 framing** interface configuration command. To return the frame type to the default, use the **no** form of this command.

### T1

```
ces dsx1 framing {esf | sf}
```

```
no ces dsx1 framing
```

### E1

```
ces dsx1 framing {e1_crc_mfCASlt | e1_crc_mf_lt | e1_lt | e1_mfCAS_lt}
```

```
no ces dsx1 framing
```

Syntax Description	esf	sf	e1_crc_mfCASlt	e1_crc_mf_lt	e1_lt	e1_mfCAS_lt
	Configures the line type to extended super frame for T1.	Configures the line type to super frame for T1.	Configures the line type to E1 CRC with channel-associated signalling (CAS) enabled.	Configures the line type to E1 CRC with CAS disabled.	Configures the line type to E1 with CAS disabled.	Configures the line type to E1 with CAS enabled.

## ces dsx1 lbo

To configure cable length for the constant bit rate (CBR) interface, use the **ces dsx1 lbo** interface configuration command. To return the cable length to the default, use the **no** form of this command.

```
ces dsx1 lbo length
```

```
no ces dsx1 lbo
```

<b>Syntax Description</b>	<i>length</i>	Sets the cable length. Values (in feet) are <b>0_110</b> , <b>110_200</b> , <b>220_330</b> , <b>330_440</b> , <b>440_550</b> , <b>550_660</b> , <b>660_above</b> , and <b>square_pulse</b> . Values represent a range in feet.
---------------------------	---------------	--

## ces dsx1 linecode

To select the line code type for the constant bit rate (CBR) interface, use the **ces dsx1 linecode** interface configuration command. To return the line code to the default, use the **no** form of this command.

**T1**

```
ces dsx1 linecode {ami | b8zs}
```

```
no ces dsx1 linecode
```

**E1**

```
ces dsx1 linecode {ami | hdb3}
```

```
no ces dsx1 linecode
```

<b>Syntax Description</b>	<b>ami</b>	Specifies the alternate mark inversion (AMI) as the line code type. Valid for T1 and E1 interfaces.
	<b>b8zs</b>	Specifies B8ZS as the line code type. Valid for T1 interfaces. This is the default for T1.
	<b>hdb3</b>	Specifies HDB3 as the line code type. Valid for E1 interfaces. This is the default for E1.

## ces dsx1 loopback

To enable a loopback for the constant bit rate (CBR) interface, use the **ces dsx1 loopback** interface configuration command. To disable the loopback, use the **no** form of this command.

```
ces dsx1 loopback {line | noloop | payload}
```

```
no ces dsx1 loopback {line | noloop | payload}
```

Syntax Description	line	Sets the received signal to be looped at the line (does not penetrate the line).
	noloop	Sets the interface to no loop.
	payload	Sets the received signal to be looped through the device and returned.

## ces dsx1 signalmode robbedbit

To enable the signal mode as robbed bit on a constant bit rate (CBR) interface, use the **ces dsx1 signalmode robbedbit** interface configuration command. To return the signal mode to the default, use the **no** form of this command.

```
ces dsx1 signalmode robbedbit
```

```
no ces dsx1 signalmode robbedbit
```

**Syntax Description** This command has no arguments or keywords.

## ces partial-fill

To configure the number of user octets per cell for the ATM circuit emulation service (CES), use the **ces partial-fill** command in interface configuration mode. To delete the CES partial-fill value, use the **no** form of this command.

```
ces partial-fill octets
```

```
no ces partial-fill octets
```

Syntax Description	<i>octets</i>	Number of user octets per cell for the CES. Possible values of octet range from 0 to 47. Setting this number to zero disables partial cell fill and causes all cells to be completely filled before they are sent.
--------------------	---------------	--

## ces pvc

To configure the destination port for the circuit on the constant bit rate (CBR) interface, use the **ces pvc** interface configuration command. To remove the destination port on the circuit, use the **no** form of this command.

```
ces pvc circuit-number interface atm slot/port vpi number vci number
```

```
no ces pvc circuit-number interface atm slot/port vpi number vci number
```

**Syntax Description**

<i>circuit-number</i>	Selects the circuit identification. The range is 0 to 24. For unstructured service, use 0. For T1 structure service, the range is 1 through 24. For E1 structure service, the range is 1 through 31.
<b>interface atm</b> <i>slot/port</i>	Slot and port number of the ATM interface. Used to create a hard permanent virtual circuit (PVC). Only a hard PVC can be configured for the CBR interfaces on the ATM-CES port adapter.
<b>vpi</b> <i>number</i>	Virtual path identifier of the destination PVC. Range is 0 through 255.
<b>vci</b> <i>number</i>	Virtual channel identifier of the destination PVC. Range is 1 through 16383.

## class-int

To assign a virtual circuit (VC) class to an ATM main interface or subinterface, use the **class-int** command in interface configuration mode. To remove a VC class, use the **no** form of this command.

**class-int** *vc-class-name*

**no class-int** *vc-class-name*

**Syntax Description**

<i>vc-class-name</i>	Name of the VC class you are assigning to your ATM main interface or subinterface.
----------------------	--

## class-vc

To assign a virtual circuit (VC) class to an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or VC bundle member, use the **class-vc** command in the appropriate configuration mode. To remove a VC class, use the **no** form of this command.

**class-vc** *vc-class-name*

**no class-vc** *vc-class-name*

**Syntax Description**

<i>vc-class-name</i>	Name of the VC class you are assigning to your ATM PVC, SVC, or VC bundle member.
----------------------	---

## dxl map

To map a protocol address to a given virtual path identifier (VPI) and virtual channel identifier (VCI), use the **dxl map** interface configuration command. To remove the mapping for that protocol and protocol address, use the **no** form of this command.

**dxl map** *protocol protocol-address vpi vci* [**broadcast**]

**no dxl map** *protocol protocol-address*

<b>Syntax Description</b>	<i>protocol</i>	One of the following bridging or protocol keywords: <b>apollo</b> , <b>appletalk</b> , <b>bridge</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , <b>novell</b> , <b>vines</b> , or <b>xns</b> .
	<i>protocol-address</i>	Protocol-specific address.
	<i>vpi</i>	Virtual path identifier in the range 0 to 15.
	<i>vci</i>	Virtual circuit identifier in the range 0 to 63.
	<b>broadcast</b>	(Optional) Address to which broadcasts should be forwarded.

## dxi pvc

To configure multiprotocol or single protocol ATM-Data Exchange Interface (DXI) encapsulation, use the **dxi pvc** interface configuration command. To disable multiprotocol ATM-DXI encapsulation, use the **no** form of this command.

```
dxi pvc vpi vci [snap | nlpid | mux]
```

```
no dxi pvc vpi vci [snap | nlpid | mux]
```

<b>Syntax Description</b>	<i>vpi</i>	ATM network virtual path identifier (VPI) of this PVC, in the range from 0 through 255. The VPI is an 8-bit field in the header of the ATM cell. The VPI value is unique only on a single interface, not throughout the ATM network, because it has local significance only.  Both <i>vpi</i> and <i>vci</i> cannot be specified as 0; if one is 0, the other cannot be 0.
	<i>vci</i>	ATM network virtual channel identifier (VCI) of this PVC, in the range from 0 through 65535. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single interface, not throughout the ATM network, because it has local significance only.  Both <i>vpi</i> and <i>vci</i> cannot be specified as 0; if one is 0, the other cannot be 0.
	<b>snap</b>	(Optional) LLC/SNAP encapsulation based on the protocol used in the packet. This keyword defines a PVC that can carry multiple network protocols. This is the default.
	<b>nlpid</b>	(Optional) RFC 1294/1490 encapsulation. This option is provided for backward compatibility with the default encapsulation in earlier versions of the Cisco IOS software.
	<b>mux</b>	(Optional) MUX encapsulation; the carried protocol is defined by the <b>dxi map</b> command when the PVC is set up. This keyword defines a PVC that carries only one network protocol.

## encapsulation aal5

To configure the ATM adaptation layer (AAL) and encapsulation type for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), virtual circuit (VC) class, or VC bundle, use the **encapsulation aal5** command in the appropriate command mode. To remove an encapsulation from a PVC, SVC, VC class, or VC bundle, use the **no** form of this command.

```
encapsulation aal5encap [virtual-template number]
```

```
no encapsulation aal5encap [virtual-template number]
```

**Note**

To configure Integrated Local Management Interface (ILMI), QSAAL, or Switched Multimegabit Data Service (SMDS) encapsulations for an ATM PVC, use the **pvc** command.

**Syntax Description***encap*

AAL and encapsulation type. When **mux** is specified, a protocol is required. Possible options for the *encap* argument are as follows:

**auto**—For PPP over ATM SVCs only. The **auto** keyword enables an ATM SVC to use either aal5snap or aal5mux encapsulation.

**ciscopp**—For Cisco Point-to-Point Protocol (PPP) over ATM. Supported on ATM PVCs only.

**mux apollo**—For a multiplex (MUX)-type VC using the Apollo protocol.

**mux appletalk**—For a MUX-type VC using the AppleTalk protocol.

**mux decnet**—For a MUX-type VC using the DECnet protocol.

**mux frame-relay**—For a MUX-type virtual circuit for Frame Relay-ATM Network Interworking (FRF.5) on the Cisco MC3810.

**mux fr-atm-srv**—For a MUX-type virtual circuit for Frame Relay-ATM Service Interworking (FRF.8) on the Cisco MC3810.

**mux ip**—For a MUX-type VC using the IP protocol.

**mux ipx**—For a MUX-type VC using the IPX protocol.

**mux ppp**—For a MUX-type virtual circuit running IETF-compliant PPP over ATM. You must use the **virtual-template** *number* argument to identify the virtual template. (If you need to establish a virtual template, use the **interface virtual-template** command.) The **mux ppp** keyword applies to ATM PVCs only.

## encapsulation atm-dxi

To enable ATM-Data Exchange Interface (DXI) encapsulation, use the **encapsulation atm-dxi** interface configuration command. To disable ATM-DXI, use the **no** form of this command.

**encapsulation atm-dxi**

**no encapsulation atm-dxi**

**Syntax Description**

This command has no arguments or keywords.

## idle-timeout

To configure the idle timeout parameter for tearing down an ATM switched virtual circuit (SVC) connection, use the **idle-timeout** command in the appropriate command mode. To disable the timeout parameter, use the **no** form of this command.

**idle-timeout** *seconds* [*minimum-rate*]

**no idle-timeout** *seconds* [*minimum-rate*]

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds that the SVC is idle, after which the ATM SVC is disconnected.
	<i>minimum-rate</i>	(Optional) Minimum traffic rate, in kilobits per second (kbps), required on an ATM SVC to maintain the SVC connection.

## ilmi manage

To enable Integrated Local Management Interface (ILMI) management on an ATM permanent virtual circuit (PVC), use the **ilmi manage** command in the appropriate command mode. To disable ILMI management, use the **no** form of this command.

**ilmi manage**

**no ilmi manage**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## ima active-links-minimum

To set the minimum number of links that must be operating in order for an ATM inverse multiplexing over ATM (IMA) group to remain in service, use the **ima active-links-minimum** interface configuration command. To remove the current configuration and set the value to the default, use the **no** form of this command.

**ima active-links-minimum** *number*

**no ima active-links-minimum** *number*

<b>Syntax Description</b>	<i>number</i>	Number of links; a value from 1 to 8.
---------------------------	---------------	---------------------------------------

## ima clock-mode

To set the transmit clock mode for an ATM inverse multiplexing over ATM (IMA) group, use the **ima clock-mode** interface configuration command. To remove the current configuration, use the **no** form of this command.

```
ima clock-mode {common port | independent}
```

```
no ima clock-mode
```

Syntax Description	common	<i>port</i>	independent
	The transmit clocks for all the links in the group are derived from the same source.	When you choose a common clock source, also specify the link that will provide clocking for the IMA group, which is called the common link. If the common link fails, the system automatically chooses one of the remaining active links to provide clocking.	The transmit clock source for at least one link in the IMA group is different from the clock source used by the other links.

## ima differential-delay-maximum

To specify the maximum differential delay among the active links in an inverse multiplexing over ATM (IMA) group, use the **ima differential-delay-maximum** interface configuration command. To restore the default setting, use the **no** form of this command.

```
ima differential-delay-maximum msec
```

```
no ima differential-delay-maximum msec
```

Syntax Description	<i>msec</i>
	Specifies the differential delay in milliseconds (ms). For T1, the range is from 25 to 250 milliseconds. For E1, the range is from 25 to 190 milliseconds.

## ima frame-length

To specify the number of cells in IMA frames, use the **ima frame-length** interface configuration command. IMA frames are numbered sequentially and each contains an IMA Control Protocol (ICP) cell at a specific position. To remove the current setting and restore the default value, use the **no** form of this command.

```
ima frame-length {32 | 64 | 128 | 256}
```

```
no ima frame-length {32 | 64 | 128 | 256}
```

Syntax Description	32	64
	Specifies a value of 32 cells.	Specifies a value of 64 cells.

<b>128</b>	Specifies a value of 128 cells.
<b>256</b>	Specifies a value of 256 cells.

## ima-group

To define physical links as inverse multiplexing over ATM (IMA) group members, use the **ima-group** interface configuration command for each group member. To remove the port from the group, use the **no** form of this command.

**ima-group** *group-number*

**no ima-group** *group-number*

### Syntax Description

<i>group-number</i>	Specifies an IMA group number from 0 to 3. IMA groups can span multiple ports on a port adapter but cannot span port adapters.
---------------------	--

## ima test

To specify an interface and test pattern for verifying connectivity of all links in an IMA group, use the **ima test** interface configuration command. To stop the test, use the **no** form of this command.

**ima test** [**link** *port*] [**pattern** *pattern-id*]

**no ima test** [**link** *port*] [**pattern** *pattern-id*]

### Syntax Description

<b>link</b> <i>port</i>	(Optional) The identifier for the interface where the physical link is located.
<b>pattern</b> <i>pattern-id</i>	(Optional) A value from 0 to 254, set in hexadecimal or decimal numbers, identifying a pattern to be sent to the far end of the link.

## inarp

To configure the Inverse Address Resolution Protocol (ARP) time period for an ATM permanent virtual circuit (PVC), virtual circuit (VC) class, or VC bundle, use the **inarp** command in the appropriate command mode. To restore the default Inverse ARP time period behavior, use the **no** form of this command.

**inarp** *minutes*

**no inarp** *minutes*

### Syntax Description

<i>minutes</i>	Number of minutes for the Inverse ARP time period.
----------------	--

# interface atm

To configure an ATM interface type and enter interface configuration mode, use the **interface atm** global configuration command.

**Cisco 7500 series with AIP; Cisco 7200 series with ATM, ATM-CES, and enhanced ATM port adapters; Cisco 2600 and 3600 series with 1-port ATM-25 network module**

```
interface atm slot/0
```

**Cisco 7500 series with ATM and enhanced ATM port adapter**

```
interface atm slot/port-adapter/0
```

**Cisco 4500 and 4700 series with NPM**

```
interface atm number
```

**Cisco 2600 and 3600 series**

```
interface atm slot/port
```

To configure an ATM subinterface, use the **interface atm** global configuration command.

**Cisco 7500 series with AIP; Cisco 7200 series with ATM, ATM-CES, and enhanced ATM port adapters; Cisco 2600 and 3600 series with 1-port ATM-25 network module**

```
interface atm slot/0.subinterface-number {multipoint | point-to-point}
```

**Cisco 7500 series with ATM and enhanced ATM port adapter**

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

**Cisco 4500 and 4700 series with NPM**

```
interface atm number.subinterface-number {multipoint | point-to-point}
```

**Cisco 2600 and 3600 series**

```
interface atm slot/port.subinterface-number {multipoint | point-to-point}
```

## Syntax Description

<i>slot</i>	Specifies the backplane slot number on your router. The value ranges from 0 to 4, depending on what router you are configuring. Refer to your router hardware documentation.
<i>/0</i>	ATM port number. Because the ATM Interface Processor (AIP) and all ATM port adapters have a single ATM interface, the port number is always 0.
<i>port-adapter</i>	ATM port adapter number for the ATM port adapter or enhanced ATM port adapter on Cisco 7500 series routers. The value can be 0 or 1.

<i>number</i>	On Cisco 4500 and Cisco 4700 routers, specifies the network processing module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the <b>show interfaces</b> command.
<i>port</i>	ATM port number on a Cisco 2600 or 3600 series router, indicating the T1 or E1 link that you are configuring. Enter a value from 0 to 3 or from 0 to 7, depending on whether the network module has four ports or eight ports.
<i>.subinterface-number</i>	Subinterface number in the range 1 to 4294967293.
<b>multipoint   point-to-point</b>	Specifies a multipoint or point-to-point subinterface.

## interface atm ima

To configure an inverse multiplexing over ATM (IMA) group, use the **interface atm ima** global configuration command. To remove the IMA group from the specified interface and remove all configurations and connections for the IMA group, use the **no** form of this command.

**interface atm** *slot/imagroup-number*

**no interface atm** *slot/imagroup-number*

<b>Syntax Description</b>	<i>slot</i>	Specifies the slot location of the ATM IMA network module. The values range from 0 to 5 depending on the router.
	<i>group-number</i>	Enter an IMA group number from 0 to 3. You can create up to four groups. Do not include a space before the group number.

## interface cbr

To specify the T1 or E1 constant bit rate interface on an ATM-CES port adapter, and to enter interface configuration mode, use the **interface cbr** global configuration command.

**interface cbr** *slot/port*

<b>Syntax Description</b>	<i>slot</i>	Backplane slot number.
	<i>port</i>	Interface port number.

# loopback

To loop packets back to the interface for testing, use the **loopback** interface configuration command with or without an optional keyword. To remove the loopback, use the **no** form of this command.

## Cisco 2600 and 3600 Series

```
loopback [line | local | payload | remote]
```

```
no loopback [line | local | payload | remote]
```

## Cisco 7100, 7200, and 7500 Series

```
loopback {diagnostic | local {payload | line} | remote {iboc | esf {payload | line}}}
```

(for T1 lines)

```
loopback {diagnostic | local {payload | line}}
```

(for E1 lines)

```
no loopback
```

### Syntax Description

<b>line</b>	Places the interface into external loopback mode at the line.
<b>local</b>	Places the interface into local loopback mode.
<b>payload</b>	Places the interface into external loopback mode at the payload level.
<b>remote</b>	Keeps the local end of the connection in remote loopback mode.
<b>diagnostic</b>	Loops the outgoing transmit signal back to the receive signal.
<b>iboc</b>	Sends an in-band code to the far-end receiver to cause it to go into line loopback.
<b>esf</b>	Specifies the FDL loopbacks. FDL should be configured on the link.

# loopback (ATM)

To configure the ATM interface into loopback mode, use the **loopback** interface configuration command. To remove the loopback, use the **no** form of this command.

```
loopback [cell | line | payload]
```

```
no loopback [cell | line | payload]
```

### Syntax Description

<b>cell</b>	(Optional) Places the interface into external loopback at cell level.
<b>line</b>	(Optional) Places the interface into external loopback at the line.
<b>payload</b>	(Optional) Places the interface into external loopback at the payload level.

## map-class atm

This command is no longer supported.

## mid

To set the range of message identifier (MID) values on a permanent virtual circuit (PVC), use the **mid** interface-ATM-VC configuration command. To remove MID value range settings, use the **no** form of this command.

**mid** *midlow midhigh*

**no mid** *midlow midhigh*

Syntax Description		
<i>midlow</i>		Starting MID number for this PVC. This can be set between 0 and 1023.
<i>midhigh</i>		Ending MID number for this PVC. This can be set between 0 and 1023.

## network-clock-select (ATM)

To establish the sources and priorities of the requisite clocking signals for an ATM-CES port adapter, use the **network-clock-select** global configuration command. To remove the clock source, use the **no** form of this command.

**network-clock-select** *priority {cbr | atm} slot/port*

**no network-clock-select** *priority {cbr | atm} slot/port*

Syntax Description		
<i>priority</i>		Priority of the clock source. Values are 1 (high priority) to 4 (low priority).
<b>cbr</b>		Specifies a CBR interface to supply the clock source.
<b>atm</b>		Specifies an ATM interface to supply the clock source.
<i>slot/</i>		Backplane slot number.
<i>port</i>		Interface port number.

## oam-pvc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC) or virtual circuit (VC) class, use the **oam-pvc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

**oam-pvc** [**manage**] [*frequency*]

**no oam-pvc** [**manage**] [*frequency*]

### Syntax Description

<b>manage</b>	(Optional) Enable OAM management.
<i>frequency</i>	(Optional) Time delay (0 to 600 seconds) between transmitting OAM loopback cells.

## oam retry

To configure parameters related to Operation, Administration, and Maintenance (OAM) management for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle, use the **oam retry** command in the appropriate command mode. To remove OAM management parameters, use the **no** form of this command.

**oam retry** *up-count down-count retry-frequency*

**no oam retry** *up-count down-count retry-frequency*

### Syntax Description

<i>up-count</i>	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a PVC connection state to up. This argument does not apply to SVCs.
<i>down-count</i>	Number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change a PVC state to down or tear down an SVC connection.
<i>retry-frequency</i>	The frequency (in seconds) that end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state of a PVC or SVC is being verified. For example, if a PVC is up and a loopback cell response is not received after the <i>frequency</i> (in seconds) argument is specified using the <b>oam-pvc</b> command, then loopback cells are sent at the <i>retry-frequency</i> to verify whether the PVC is down.

## oam-svc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM switched virtual circuit (SVC) or virtual circuit (VC) class, use the **oam-svc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

**oam-svc** [**manage**] [*frequency*]

**no oam-svc** [**manage**] [*frequency*]

---

### Syntax Description

**manage** (Optional) Enable OAM management.

*frequency* (Optional) Time delay (0 to 600 seconds) between transmitting OAM loopback cells.

---

## partial-fill

To configure the number of AAL1 user octets per cell for the ATM circuit emulation service (CES) on the OC-3/STM-1 Circuit Emulation Service network module, use the **partial-fill** interface-CES-VC command. To delete the CES partial-fill value, use the **no** form of this command.

**partial-fill** *octet*

**no partial-fill** *octet*

---

### Syntax Description

*octet* Number of user octets per cell for the CES. Possible values of octet range from 1 to 47.

---

## protocol (ATM)

To configure a static map for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or VC class or to enable Inverse Address Resolution Protocol (ARP) or Inverse ARP broadcasts on an ATM PVC, use the **protocol** command in the appropriate command mode. To remove a static map or disable Inverse ARP, use the **no** form of this command.

**protocol** *protocol* {*protocol-address* | **inarp**} [[**no**] **broadcast**]

**no protocol** *protocol* {*protocol-address* | **inarp**} [[**no**] **broadcast**]

**Syntax Description**

<i>protocol</i>	Choose one of the following keywords: <b>aarp</b> —AppleTalk ARP <b>apollo</b> —Apollo domain <b>appletalk</b> —AppleTalk <b>arp</b> —IP ARP <b>bridge</b> —bridging <b>bstun</b> —block serial tunnel <b>cdp</b> —Cisco Discovery Protocol <b>clns</b> —ISO Connectionless Network Service (CLNS) <b>clns_es</b> —ISO CLNS end system <b>clns_is</b> —ISO CLNS intermediate system <b>cmns</b> —ISO CMNS <b>compressedtcp</b> —Compressed TCP <b>decnet</b> —DECnet <b>decnet_node</b> —DECnet node <b>decnet_prime_router</b> —DECnet prime router <b>decnet_router-l1</b> —DECnet router L1 <b>decnet_router-l2</b> —DECnet router L2 <b>dls</b> —data link switching <b>ip</b> —IP <b>ipx</b> —Novell IPX <b>llc2</b> —llc2 <b>pad</b> —packet assembler/disassembler (PAD) links <b>pppoe</b> —PPP over Ethernet <b>qlc</b> —Qualified Logical Link Control protocol <b>rsrb</b> —remote source-route bridging <b>snapshot</b> —snapshot routing support <b>stun</b> —serial tunnel <b>vines</b> —Banyan VINES <b>xns</b> —Xerox Network Systems protocol
<i>protocol-address</i>	Destination address that is being mapped to a PVC.
<b>inarp</b>	(Valid only for IP and IPX protocols on PVCs) Use this keyword to enable Inverse ARP on an ATM PVC. If you specify a <i>protocol-address</i> instead of <b>inarp</b> , Inverse ARP is automatically disabled for that protocol.
<b>[no] broadcast</b>	(Optional) <b>broadcast</b> indicates that this map entry is used when the corresponding protocol sends broadcast packets to the interface. Pseudobroadcasting is supported. The <b>broadcast</b> keyword of the <b>protocol</b> command takes precedence if you previously configured the <b>broadcast</b> command on the ATM PVC or SVC.

## pvc

To create or assign a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC, and to enter interface-ATM-VC configuration mode, use the **pvc** command in interface or subinterface configuration mode. To remove an ATM PVC, use the **no** form of this command.

```
pvc [name] vpi/vci [ces | ilmi | qsaal | smds]
```

```
no pvc [name] vpi/vci [ces | ilmi | qsaal | smds]
```

Syntax Description	
<i>name</i>	(Optional) The name of the PVC or map. The name can be up to 16 characters long.
<i>vpi</i>	<p>ATM network virtual path identifier (VPI) for this PVC. The absence of the “/” and a <i>vpi</i> value defaults the <i>vpi</i> value to 0.</p> <p>On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255; on the Cisco 4500 and 4700 routers, this value ranges from 0 to 1 less than the quotient of 8192 divided by the value set by the <b>atm vc-per-vc</b> command; on 2600 and 3600 series routers using Inverse Multiplexing for ATM (IMA), the ranges are 0 to 15, 64 to 79, 128 to 143, and 192 to 207.</p> <p>The arguments <i>vpi</i> and <i>vci</i> cannot both be set to 0; if one is 0, the other cannot be 0.</p>
<i>vci</i>	<p>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 <b>atm vc-per-vc</b> command. Typically, lower values 0 to 31 are reserved for specific traffic (for example, F4 OAM, SVC signalling, ILMI, and so on) and should not be used.</p> <p>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.</p> <p>The arguments <i>vpi</i> and <i>vci</i> cannot both be set to 0; if one is 0, the other cannot be 0.</p>
<b>ces</b>	(Optional) Circuit Emulation Service encapsulation. This keyword is available on the OC-3/STM-1 ATM Circuit Emulation Service network module only.
<b>ilmi</b>	(Optional) Used to set up communication with the Interim Local Management Interface (ILMI); the associated <i>vpi</i> and <i>vci</i> values ordinarily are 0 and 16, respectively.
<b>qsaal</b>	(Optional) A signalling-type PVC used for setting up or tearing down SVCs; the associated <i>vpi</i> and <i>vci</i> values ordinarily are 0 and 5, respectively.
<b>smds</b>	(Optional) Encapsulation for SMDS networks. If you are configuring an ATM PVC on the ATM Interface Processor (AIP), you must configure AAL3/4SMDS using the <b>atm aal aal3/4</b> command before specifying <b>smds</b> encapsulation. If you are configuring an ATM network processor module (NPM), the <b>atm aal aal3/4</b> command is not required. SMDS encapsulation is not supported on the ATM port adapter.

## retry

To configure a router to periodically attempt to bring up an active SVC connection after the initial call setup failed, use the **retry** interface-CES-VC command. To disable the retry mechanism, use the **no** form of this command.

```
retry timeout_value [retry_limit] [first_retry_interval]
```

```
no retry
```

Syntax Description		
<i>timeout_value</i>		Number of seconds between attempts to bring up the connection. The range is from 1 to 86400 seconds.
<i>retry_limit</i>		(Optional) Number of attempts the router will make to bring up the connection. The range is from 0 to 65535. The default value of 0 indicates no limit.
<i>first_retry_interval</i>		(Optional) Number of seconds the router will wait after the first call attempt failed before trying the call again. The default is 10 seconds.

## scrambling cell-payload

To improve data reliability by randomizing the ATM cell payload frames on Cisco 7100, 7200, or 7500 series routers, use the **scrambling cell-payload** interface configuration command. To disable scrambling, use the **no** form of this command.

```
scrambling cell-payload
```

```
no scrambling cell-payload
```

**Syntax Description** This command has no arguments or keywords.

## scrambling-payload

To improve data reliability by randomizing the ATM cell payload frames on Cisco 2600 or 3600 series routers, use the **scrambling-payload** interface configuration command. To disable scrambling, use the **no** form of this command.

```
scrambling-payload
```

```
no scrambling-payload
```

**Syntax Description** This command has no arguments or keywords.

## show atm arp-server

To display the ATM Address Resolution Protocol (ARP) server's information about one specific interface or all interfaces, use the **show atm arp-server** user EXEC command.

**AIP on Cisco 7500 series with AIP; Cisco 7200 series with ATM, ATM-CES, and enhanced ATM port adapters; Cisco 2600 and 3600 series with 1-port ATM-25 network module**

```
show atm arp-server [atm slot/port[.subinterface-number]]
```

**Cisco 7500 series with ATM and enhanced ATM port adapters**

```
show atm arp-server [atm slot/port-adapter/port[.subinterface-number]]
```

**Cisco 4500 and 4700 series with NPM**

```
show atm arp-server [atm number[.subinterface-number]]
```

Syntax Description		
<b>atm slot/port</b>	(Optional) ATM slot and port numbers. Use this format for the following platform configurations:	<ul style="list-style-type: none"> <li>AIP on Cisco 7500 series routers.</li> <li>ATM port adapter, ATM-CES port adapter, and enhanced ATM port adapter on Cisco 7200 series routers.</li> <li>1-port ATM-25 network module on Cisco 2600 and 3600 series routers.</li> </ul>
<b>atm slot/port-adapter/port</b>	(Optional) ATM slot, port adapter, and port numbers. Use this format for the ATM port adapter or enhanced ATM port adapter on Cisco 7500 series routers.	
<b>atm number</b>	(Optional) ATM network processor module (NPM) number on Cisco 4500 and 4700 routers.	
<b>.subinterface-number</b>	(Optional) Subinterface number.	

## show atm class-links

To display virtual circuit (VC) parameter configurations and where the parameter values are inherited from, use the **show atm class-links** privileged EXEC command.

```
show atm class-links {vpi/vci | name}
```

Syntax Description		
<b>vpi/vci</b>	The ATM VPI and VCI numbers. The absence of the slash character (/) and a vpi value defaults the vpi value to 0.	
<b>name</b>	Name of the VC.	

## show atm interface atm

To display ATM-specific information about an ATM interface, use the **show atm interface atm** privileged EXEC command.

**Cisco 7500 series with AIP; Cisco 7200 series with ATM, ATM-CES, and enhanced ATM port adapters; Cisco 2600 and 3600 series with 1-port ATM-25 network module**

```
show atm interface atm slot/port
```

**Cisco 7500 series with ATM and enhanced ATM port adapters**

```
show atm interface atm slot/port-adapter/port
```

**Cisco 4500 and 4700 series with NPM**

```
show atm interface atm number
```

Syntax	Description
<i>slot/port</i>	ATM slot number and port number. Use this format on the following platform configurations: <ul style="list-style-type: none"> <li>The AIP on Cisco 7500 series routers.</li> <li>The ATM port adapter, ATM-CES port adapter, or enhanced ATM port adapter on Cisco 7200 series routers.</li> <li>The 1-port ATM-25 network module on Cisco 2600 and 3600 series routers.</li> </ul>
<i>slot/port-adapter/port</i>	ATM slot, port adapter, and port number. Use this format on the ATM port adapter or ATM-CES port adapter on Cisco 7500 series routers.
<i>number</i>	NPM number for Cisco 4500 and 4700 routers.

## show atm map

To show the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps, use the **show atm map** privileged EXEC command.

```
show atm map
```

Syntax	Description
	This command has no arguments or keywords.

## show atm pvc

To display all ATM permanent virtual connections (PVCs) and traffic information, use the **show atm pvc** privileged EXEC command.

```
show atm pvc [vpi/vci | name | interface atm interface-number][ppp]
```

Syntax	Description
<i>vpi/vci</i>	(Optional) The ATM virtual path identifier (VPI) and virtual channel identifier (VCI) numbers. The absence of the slash character (/) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0.
<i>name</i>	(Optional) Name of the PVC.
<b>interface atm</b> <i>interface-number</i>	(Optional) Interface number or subinterface number of the PVC. Displays all PVCs on the specified interface or subinterface.  The <i>interface-number</i> argument uses one of the following formats, depending on which router platform you are using: <ul style="list-style-type: none"> <li>For the ATM Interface Processor (AIP) on Cisco 7500 series routers; for the ATM port adapter, ATM-CES port adapter, and enhanced ATM port adapter on Cisco 7200 series routers; for the 1-port ATM-25 network module on Cisco 2600 and Cisco 3600 series routers: <i>slot/0</i>[<i>.subinterface-number multipoint</i>]</li> <li>For the ATM port adapter and enhanced ATM port adapter on Cisco 7500 series routers: <i>slot/port-adapter/0</i>[<i>.subinterface-number multipoint</i>]</li> <li>For the NPM on Cisco 4500 and 4700 routers: <i>number</i>[<i>.subinterface-number multipoint</i>]</li> </ul> For a description of these arguments, refer to the <b>interface atm</b> command.
<b>ppp</b>	(Optional) Displays each PVC configured for PPP over ATM.

## show atm svc

To display all ATM switched virtual circuits (SVCs) and traffic information, use the **show atm svc** privileged EXEC command.

```
show atm svc [vpi/vci | name | interface atm interface-number]
```

<b>Syntax Description</b>	<i>vpi/vci</i>	(Optional) The ATM VPI and VCI numbers. The absence of the slash character (/) and a <i>vpi</i> value defaults the <i>vpi</i> value to 0.
	<i>name</i>	(Optional) Name of the SVC.
	<b>interface atm</b> <i>interface-number</i>	(Optional) Interface number or subinterface number of the SVC. Displays all SVCs on the specified interface or subinterface.  The <i>interface-number</i> argument uses one of the following formats, depending on what router platform you are using: <ul style="list-style-type: none"> <li>For the AIP on Cisco 7500 series routers; For the ATM port adapter, ATM-CES port adapter, and enhanced ATM port adapter on Cisco 7200 series routers; For the 1-port ATM-25 network module on Cisco 2600 and 3600 series routers: <i>slot/0[.subinterface-number multipoint]</i></li> <li>For the ATM port adapter and enhanced ATM port adapter on Cisco 7500 series routers: <i>slot/port-adapter/0[.subinterface-number multipoint]</i></li> <li>For the NPM on Cisco 4500 and 4700 routers: <i>number[.subinterface-number multipoint]</i></li> </ul> For a description of these arguments, refer to the <b>interface atm</b> command.

## show atm traffic

To display current, global ATM traffic information to and from all ATM networks connected to the router, use the **show atm traffic** privileged EXEC command.

```
show atm traffic
```

**Syntax Description** This command has no arguments or keywords.

## show atm vc

To display all ATM permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) and traffic information, use the **show atm vc** privileged EXEC command.

```
show atm vc [vcd | interface interface-number]
```

<b>Syntax Description</b>	<i>vcd</i>	(Optional) Specifies which virtual circuit about which to display information.
<b>interface</b> <i>interface-number</i>		(Optional) Interface number or subinterface number of the PVC or SVC. Displays all PVCs and SVCs on the specified interface or subinterface.  The <i>interface-number</i> uses one of the following formats, depending on what router platform you are using: <ul style="list-style-type: none"> <li>• For the ATM Interface Processor (AIP) on Cisco 7500 series routers; for the ATM port adapter, ATM-CES port adapter, and enhanced ATM port adapter on Cisco 7200 series routers; For the 1-port ATM-25 network module on Cisco 2600 and 3600 series routers: <i>slot/0[.subinterface-number multipoint]</i></li> <li>• For the ATM port adapter and enhanced ATM port adapter on Cisco 7500 series routers: <i>slot/port-adapter/0[.subinterface-number multipoint]</i></li> <li>• For the network processing module (NPM) on Cisco 4500 and 4700 routers: <i>number[.subinterface-number multipoint]</i></li> </ul> For a description of these arguments, refer to the <b>interface atm</b> command.

## show atm vp

To display the statistics for all virtual paths (VPs) on an interface or for a specific VP, use the **show atm vp** privileged EXEC command.

```
show atm vp [vpi]
```

<b>Syntax Description</b>	<i>vpi</i>	(Optional) ATM network virtual path identifier (VPI) of the permanent virtual path. The range is 0 to 255. The VPI is an 8-bit field in the header of the ATM cell.
---------------------------	------------	---

## show ces

To display details about a Circuit Emulation Service (CES) connection, use the **show ces** privileged EXEC command.

```
show ces [slot/port]
```

<b>Syntax Description</b>	<i>slot/port</i>	(Optional) Slot and port number of the CES interface.
---------------------------	------------------	---

## show ces circuit

To display detailed circuit information for the constant bit rate (CBR) interface, use the **show ces circuit** privileged EXEC command.

```
show ces circuit [interface cbr slot/port [circuit-number]]
```

Syntax Description	interface cbr slot/port	(Optional) Slot and port number of the CBR interface.
	circuit-number	(Optional) Circuit identification. For unstructured service, use 0. For T1 structure service, the range is 1 through 24. For E1 structure service, the range is 1 through 31.

## show ces interface cbr

To display detailed constant bit rate (CBR) port information, use the **show ces interface cbr** privileged EXEC command.

```
show ces interface cbr slot/port
```

Syntax Description	slot/port	Slot and port number of the CES interface.
--------------------	-----------	--

## show ces status

To display the status of the ports on the ATM-CES port adapter, use the **show ces status** privileged EXEC command.

```
show ces status
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

## show controllers atm

To display information about an inverse multiplexing over ATM (IMA) group, use the **show controllers atm** privileged EXEC command.

**Cisco 2600 and 3600 Series**

```
show controllers atm [slot/ima group-number]
```

**Cisco 7200 Series**

```
show controller atm [slot/port]
```

or

```
show controllers atm [slot/imagroup-number]
```

**Cisco 7500 Series** (physical port hardware information)

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

**Cisco 7500 Series** (IMA group hardware information)

```
show controllers atm [slot/port-adapter/imagroup-number]
```

Syntax Description	
<i>slot</i>	(Optional) ATM slot number.
<b>ima</b>	(Optional) This keyword indicates an IMA group specification rather than a port value for a UNI interface.
<i>group-number</i>	(Optional) Enter an IMA group number from 0 to 3. If you specify the group number, do not insert a space between <b>ima</b> and the number.
<i>port</i>	(Optional) ATM port number.
<i>port-adapter/</i>	(Optional) ATM port adapter.

## show dxi map

To display all the protocol addresses mapped to a serial interface, use the **show dxi map EXEC** command.

```
show dxi map
```

**Syntax Description** This command has no arguments or keywords.

## show dxi pvc

To display the permanent virtual circuit (PVC) statistics for a serial interface, use the **show dxi pvc EXEC** command.

```
show dxi pvc
```

**Syntax Description** This command has no arguments or keywords.

## show ima interface atm

To display information about all configured inverse multiplexing over ATM (IMA) groups or a specific group, use the **show ima interface atm** privileged EXEC command.

### Cisco 2600 and 3600 Series

```
show ima interface atm [slot/imagroup-number] [detail]
```

### Cisco 7200 Series

```
show ima interface atm [slot/port] [detail]
```

or

```
show ima interface atm [slot/port-adapter/imagroup-number] [detail]
```

### Cisco 7500 Series

```
show ima interface atm [slot/port-adapter/slot] [detail]
```

or

```
show ima interface atm [slot/port-adapter/imagroup-number] [detail]
```

### Syntax Description

<i>slot</i>	(Optional) ATM slot number.
<b>ima</b>	(Optional) This keyword indicates an IMA group specification rather than a port value for a UNI interface.
<i>group-number</i>	(Optional) Enter an IMA group number from 0 to 3. If you specify the group number, do not insert a space between <b>ima</b> and the number.
<i>port</i>	(Optional) ATM port number.
<i>port-adapter</i>	(Optional) ATM port adapter.
<b>detail</b>	(Optional) To obtain detailed information, use this keyword.

## show interface cbr

To display information about the constant bit rate (CBR) interface on the ATM-CES port adapter, use the **show interface cbr** privileged EXEC command.

```
show interface cbr
```

### Syntax Description

This command has no arguments or keywords.

## show interfaces atm

To display information about the ATM interface, use the **show interfaces atm** privileged EXEC command.

**Cisco 7500 series with AIP; Cisco 7200 series with ATM, ATM-CES, and enhanced ATM port adapter; Cisco 2600 and 3600 series with 1-port ATM-25 network module**

```
show interfaces atm [slot/port]
```

**Cisco 7500 series routers with the ATM port adapter and enhanced ATM port adapter**

```
show interfaces atm [slot/port-adapter/port]
```

Syntax Description	
<i>slot/port</i>	(Optional) ATM slot number and port number. Use this format for the following platform configurations: <ul style="list-style-type: none"> <li>• The AIP on Cisco 7500 series routers.</li> <li>• The ATM port adapter, ATM-CES port adapter, or enhanced ATM port adapter on Cisco 7200 series routers.</li> <li>• The 1-port ATM-25 network module on Cisco 2600 and 3600 series routers.</li> </ul>
<i>slot/port-adapter/port</i>	(Optional) ATM slot, port adapter, and port numbers. Use this format for the ATM port adapter or enhanced ATM port adapter on Cisco 2600 and 3600 series routers.

## show network-clocks

To display the current configured and active network clock sources, use the **show network-clocks** privileged EXEC command.

```
show network-clocks
```

**Syntax Description** This command has no arguments or keywords.

## show sscop

To show Service-Specific Connection-Oriented Protocol (SSCOP) details for all ATM interfaces, use the **show sscop** privileged EXEC command.

```
show sscop
```

**Syntax Description** This command has no arguments or keywords.

## sscop cc-timer

To change the connection control timer, use the **sscop cc-timer** interface configuration command. To restore the default value, use the **no** form of this command.

**sscop cc-timer** *seconds*

**no sscop cc-timer**

---

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds between Begin messages.
---------------------------	----------------	---

---

## sscop keepalive-timer

To change the keepalive timer, use the **sscop keepalive-timer** interface configuration command. To restore the default value, use the **no** form of this command.

**sscop keepalive-timer** *seconds*

**no sscop keepalive-timer** *seconds*

---

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds the router waits between transmission of POLL PDUs when no sequential data (SD) or SDP PDUs are queued for transmission or are outstanding pending acknowledgments.
---------------------------	----------------	---

---

## sscop max-cc

To change the retry count of connection control, use the **sscop max-cc** interface configuration command. To restore the default value, use the **no** form of this command.

**sscop max-cc** *retries*

**no sscop max-cc**

---

<b>Syntax Description</b>	<i>retries</i>	Number of times that SSCOP will retry to transmit BGN (establishment), END (release), or RS (resynchronization) PDUs as long as an acknowledgment has not been received. Valid range is from 1 to 6000.
---------------------------	----------------	---

---

## sscop poll-timer

To change the poll timer, use the **sscop poll-timer** interface configuration command. To restore the default value, use the **no** form of this command.

**sscop poll-timer** *seconds*

**no sscop poll-timer**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds that the router waits between transmission of POLL PDUs.
---------------------------	----------------	--

## sscop receive-window

To change the receiver window, use the **sscop receive-window** interface configuration command. To restore the default value, use the **no** form of this command.

**sscop receive-window** *packets*

**no sscop receive-window**

<b>Syntax Description</b>	<i>packets</i>	Number of packets the interface can receive before it must send an acknowledgment to the ATM switch. Valid range is from 1 to 6000.
---------------------------	----------------	---

## sscop send-window

To change the transmitter window, use the **sscop send-window** interface configuration command. To restore the default value, use the **no** form of this command.

**sscop send-window** *packets*

**no sscop send-window**

<b>Syntax Description</b>	<i>packets</i>	Number of packets the interface can send before it must receive an acknowledgment from the ATM switch. Valid range is from 1 to 6000.
---------------------------	----------------	---

## SVC

To create an ATM switched virtual circuit (SVC) and specify the destination network service access point (NSAP) address on a main interface or subinterface, use the **svc** interface configuration command. To disable the SVC, use the **no** form of this command.

**svc** [*name*] [**nsap** *address*] [**ces**]

**no svc** [*name*] [**nsap** *address*] [**ces**]

**Syntax Description**

<i>name</i>	(Optional) The name of the SVC and map. The name can be up to 16 characters long. A name is required when creating a passive CES SVC.
<b>nsap</b> <i>address</i>	(Optional) The destination ATM NSAP address. Must be exactly 40 hexadecimal digits long and in the correct format. An NSAP address is required when creating an active CES SVC.
<b>ces</b>	(Optional) Circuit Emulation Service encapsulation. This keyword is available on the OC-3/STM-1 ATM Circuit Emulation Service network module only.

## ubr

To configure unspecified bit rate (UBR) quality of service (QoS) and specify the output peak cell rate (PCR) for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), virtual circuit (VC) class, or VC bundle member, use the **ubr** command in the appropriate command mode. To remove the UBR parameter, use the **no** form of this command.

```
ubr output-pcr [input-pcr]
```

```
no ubr output-pcr [input-pcr]
```

**Syntax Description**

<i>output-pcr</i>	The output PCR in kbps.
<i>input-pcr</i>	(Optional for SVCs only) The input peak cell rate (PCR) in kilobits per second. If this value is omitted, the <i>input-pcr</i> will equal the <i>output-pcr</i> .

## ubr+

To configure unspecified bit rate (UBR) quality of service (QoS) and specify the output peak cell rate and output minimum guaranteed cell rate for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), virtual circuit (VC) class, or VC bundle member, use the **ubr+** command in the appropriate command mode. To remove the UBR+ parameters, use the **no** form of this command.

```
ubr+ output-pcr output-mcr [input-pcr] [input-mcr]
```

```
no ubr+ output-pcr output-mcr [input-pcr] [input-mcr]
```

**Syntax Description**

<i>output-pcr</i>	The output peak cell rate (PCR) in kbps.
<i>output-mcr</i>	The output minimum guaranteed cell rate in kbps.
<i>input-pcr</i>	(Optional for SVCs only) The input PCR in kbps. If this value is omitted, the <i>input-pcr</i> will equal the <i>output-pcr</i> .
<i>input-mcr</i>	(Optional for SVCs only) The input minimum guaranteed cell rate in kbps. If this value is omitted, the <i>input-mcr</i> will equal the <i>output-mcr</i> .

## vbr-nrt

To configure the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specify output peak cell rate (PCR), output sustainable cell rate, and output maximum burst cell size for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), VC class, or VC bundle member, use the **vbr-nrt** command in the appropriate command mode. To remove the VBR-NRT parameters, use the **no** form of this command.

**vbr-nrt** *output-pcr output-scr output-mbs [input-pcr] [input-scr] [input-mbs]*

**no vbr-nrt** *output-pcr output-scr output-mbs [input-pcr] [input-scr] [input-mbs]*

### Syntax Description

<i>output-pcr</i>	The output PCR, in kbps.
<i>output-scr</i>	The output SCR, in kbps.
<i>output-mbs</i>	The output maximum burst cell size, expressed in number of cells.
<i>input-pcr</i>	(Optional for SVCs only) The input PCR, in kbps.
<i>input-scr</i>	(Optional for SVCs only) The input SCR, in kbps.
<i>input-mbs</i>	(Optional for SVCs only) The input maximum burst cell size, expressed in number of cells.

## vc-class atm

To create a virtual circuit (VC) class for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or ATM interface and enter vc-class configuration mode, use the **vc-class atm** global configuration command. To remove a VC class, use the **no** form of this command.

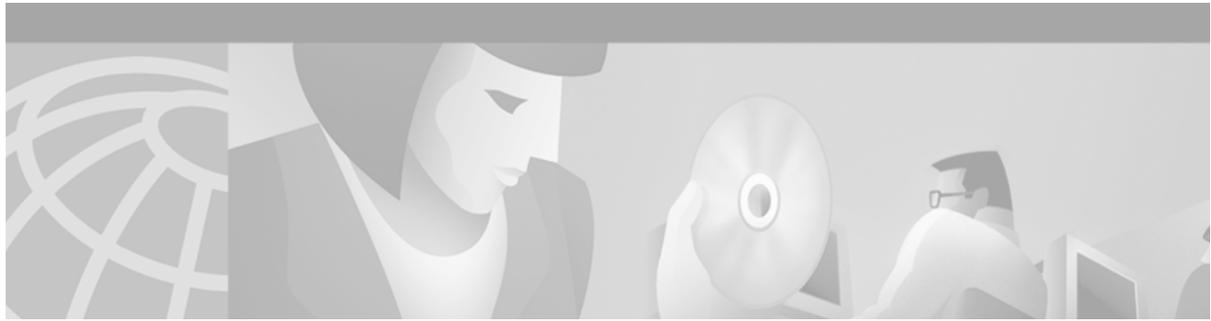
**vc-class atm** *name*

**no vc-class atm** *name*

### Syntax Description

<i>name</i>	Name of your VC class.
-------------	------------------------





## Broadband Access: PPP and Routed Bridge Encapsulation Commands

---

This chapter describes the function and syntax of the commands that configure PPP and routed bridge encapsulation for broadband access. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Wide-Area Networking Command Reference*.

### atm route-bridge

To configure an interface to use the ATM routed bridge encapsulation, use the **atm route-bridge** interface configuration command.

**atm route-bridge** *protocol*

---

#### Syntax Description

<i>protocol</i>	Protocol to be route-bridged. IP is the only protocol that can be route-bridged using ATM routed bridge encapsulation.
-----------------	--

---

### class-range

To assign a virtual circuit (VC) class to an ATM permanent virtual circuit (PVC) range, use the **class-range** PVC range configuration command. To remove the VC class, use the **no** form of this command.

**class-range** *class-name*

**no class-range** *class-name*

---

#### Syntax Description

<i>class-name</i>	Name of the VC class.
-------------------	-----------------------

---

## max bandwidth

To specify the total amount of outgoing bandwidth available to SVCs in the current configuration, use the **max bandwidth** interface-ATM-VC configuration command. To remove the current bandwidth setting, use the **no** form of this command.

**max bandwidth** *kbps*

**no max bandwidth** *kbps*

<b>Syntax Description</b>	<i>kbps</i>	Total amount of outgoing bandwidth in kilobits per second available to all SVCs in the current configuration.
---------------------------	-------------	---

## max vc

To specify the maximum number of switched virtual circuits (SVCs) that can be established using the current configuration, use the **max vc** interface-ATM-VC configuration command. To restore the maximum number of SVCs to the default setting, use the **no** form of this command.

**max vc** *number*

**no max vc** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of SVCs to be established using the current SVC configuration.
---------------------------	---------------	---

## oam-range

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC) range, use the **oam-range** PVC range configuration command. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

**oam-range** [**manage**] [*frequency*]

**no oam-range** [**manage**] [*frequency*]

<b>Syntax Description</b>	<b>manage</b>	(Optional) Enables OAM management.
	<i>frequency</i>	(Optional) Time delay (0 to 600 seconds) between transmissions of OAM loopback cells.

## pppoe enable

To enable PPP over Ethernet (PPPoE) sessions on an Ethernet interface, use the **pppoe enable** interface configuration command. To disable PPPoE, use the **no** form of this command.

**pppoe enable**

**no pppoe enable**

---

**Syntax Description** This command has no arguments or keywords.

## pppoe limit per-mac

To specify the maximum number of PPPoE sessions to be sourced from a MAC address, use the **pppoe limit per-mac** command in VPDN configuration mode.

**pppoe limit per-mac** *number*

---

**Syntax Description** *number* Maximum number of PPPoE sessions that can be sourced from a MAC address.

---

## pppoe limit per-vc

To specify the maximum number of PPPoE sessions to be established over a VC, use the **pppoe limit per-vc** command in VPDN configuration mode.

**pppoe limit per-vc** *number*

---

**Syntax Description** *number* Maximum number of PPPoE sessions that can be established over an ATM PVC.

---

## pppoe limit per-vlan

To specify the maximum number of PPP over Ethernet (PPPoE) sessions permitted under each virtual LAN (VLAN), use the **pppoe limit per-vlan** VPDN configuration command. To remove this specification, use the **no** form of this command.

**pppoe limit per-vlan** *number*

**no pppoe limit per-vlan**

Syntax Description	<i>number</i>	Maximum number of PPP over Ethernet sessions permitted under each VLAN.
--------------------	---------------	---

## pppoe max-session

To specify the maximum number of PPP over Ethernet (PPPoE) sessions permitted under a virtual LAN (VLAN), use the **pppoe max-session** Ethernet subinterface configuration command. To remove this specification, use the **no** form of this command.

**pppoe max-session** *number*

**no pppoe max-session**

Syntax Description	<i>number</i>	Maximum number of PPP over Ethernet sessions permitted under a VLAN.
--------------------	---------------	--

## pvc-in-range

To configure an individual permanent virtual circuit (PVC) within a PVC range, use the **pvc-in-range** PVC range configuration command. To delete the individual PVC configuration, use the **no** form of this command.

**pvc-in-range** [*pvc-name*] [*vpi/vci*]

**no pvc-in-range** [*pvc-name*] [*vpi/vci*]

Syntax Description	<i>pvc-name</i>	(Optional) Name given to the PVC. The PVC name can have a maximum of 15 characters.
	<i>vpi</i>	(Optional) ATM network virtual path identifier (VPI) for this PVC. In the absence of the “/” and a <i>vpi</i> value, the <i>vpi</i> value defaults to 0. The <i>vpi</i> value ranges from 0 to 255.
	<i>vci</i>	(Optional) ATM network virtual channel identifier (VCI) for this PVC. The <i>vci</i> value ranges from 32 to 2047.

## range pvc

To define a range of ATM permanent virtual circuits (PVCs), use the **range pvc** subinterface configuration command. To delete the range of ATM PVCs, use the **no** form of this command.

```
range [range-name] pvc start-vpil/start-vci end-vpil/end-vci
```

```
no range [range-name] pvc
```

Syntax Description		
	<i>range-name</i>	(Optional) Name of the range. The range name can be a maximum of 15 characters.
	<i>start-vpil</i>	Beginning value for a range of virtual path identifiers (VPIs). In the absence of the “/” and a <i>vpi</i> value, the <i>vpi</i> value defaults to 0. The <i>vpi</i> value ranges from 0 to 255.
	<i>start-vcil</i>	Beginning value for a range of virtual channel identifiers (VCIs). The <i>vci</i> value ranges from 32 to 65535.
	<i>end-vpi</i>	End value for a range of virtual path identifiers (VPIs). In the absence of an <i>end-vpi</i> value, the <i>end-vpi</i> value defaults to the <i>start-vpi</i> value. The <i>vpi</i> value ranges from 0 to 255.
	<i>end-vci</i>	End value for a range of virtual channel identifiers (VCIs). The <i>vci</i> value ranges from 32 to 65535.

## show atm svc ppp

To display information about each switched virtual circuit (SVC) configured for PPP over ATM, use the **show atm svc ppp** privileged EXEC command.

```
show atm svc ppp
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

## shutdown (PVC-in-range)

To deactivate an individual permanent virtual circuit (PVC) within a PVC range, use the **shutdown** PVC-in-range configuration command. To reactivate an individual PVC within PVC range, use the **no** form of this command.

```
shutdown
```

```
no shutdown
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

## shutdown (PVC range)

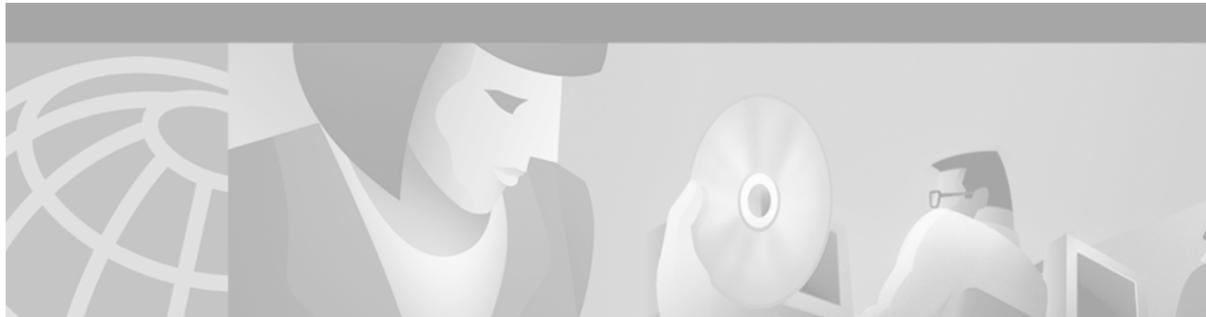
To deactivate a PVC range, use the **shutdown** PVC range configuration command. To reactivate a PVC range, use the **no** form of this command.

**shutdown**

**no shutdown**

---

**Syntax Description** This command has no arguments or keywords.



## Frame Relay Commands

---

This chapter describes the function and syntax of the Frame Relay commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Wide-Area Networking Command Reference*.

### class (map-list)

To associate a map class with a protocol-and-address combination, use the **class** map-list configuration command.

```
protocol protocol-address class map-class [broadcast] [trigger] [ietf]
```

Syntax Description	
<i>protocol</i>	Supported protocol, bridging, or logical link control keywords: <b>appletalk</b> , <b>bridging</b> , <b>clns</b> , <b>decnet</b> , <b>dls</b> , <b>ip</b> , <b>ipx</b> , <b>llc2</b> , <b>rsrb</b> , <b>vines</b> , and <b>xns</b> .
<i>protocol-address</i>	Protocol address. The <b>bridge</b> and <b>clns</b> keywords do not use protocol addresses.
<i>map-class</i>	Name of the map class from which to derive quality of service (QoS) information.
<b>broadcast</b>	(Optional) Allows broadcasts on this SVC.
<b>trigger</b>	(Optional) Enables a broadcast packet to trigger an SVC. If an SVC already exists that uses this map class, the SVC will carry the broadcast. This keyword can be configured only if <b>broadcast</b> is also configured.
<b>ietf</b>	(Optional) Specifies RFC 1490 encapsulation. The default is Cisco encapsulation.

## class (virtual circuit)

To associate a map class with a specified data-link connection identifier (DLCI), use the **class** virtual circuit configuration command. To remove the association between the DLCI and the map class, use the **no** form of this command.

**class** *name*

**no class** *name*

Syntax Description	<i>name</i>
	Name of map class to associate with this DLCI.

## clear frame-relay-inarp

To clear dynamically created Frame Relay maps, which are created by the use of Inverse Address Resolution Protocol (ARP), use the **clear frame-relay-inarp** EXEC command.

**clear frame-relay-inarp**

Syntax Description	This command has no arguments or keywords.
--------------------	--

## connect (Frame Relay)

To define connections between Frame Relay PVCs, use the **connect** global configuration command. To remove connections, use the **no** form of this command.

**connect** *connection-name interface dlc1 interface dlc1*

**no connect** *connection-name interface dlc1 interface dlc1*

Syntax Description	<i>connection-name</i>	<i>interface</i>	<i>dlci</i>
	A name for this connection.	Interface on which a PVC connection will be defined.	Data-link connection identifier (DLCI) number of the PVC that will be connected.

## encapsulation frame-relay

To enable Frame Relay encapsulation, use the **encapsulation frame-relay** interface configuration command. To disable Frame Relay encapsulation, use the **no** form of this command.

**encapsulation frame-relay** [*cisco* | *ietf*]

**no encapsulation frame-relay** [*ietf*]

Syntax Description		
	<b>cisco</b>	(Optional) Uses Cisco's own encapsulation, which is a 4-byte header, with 2 bytes to identify the data-link connection identifier (DLCI) and 2 bytes to identify the packet type.
	<b>ietf</b>	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.

## fr-atm connect dlci

To connect a Frame Relay data-link connection identifier (DLCI) to an ATM virtual circuit descriptor for FRF.5 Frame Relay-ATM Interworking (currently only available for the Cisco MC 3810), use the **fr-atm connect dlci** interface configuration command. The encapsulation type of the current interface must be Frame Relay or Frame Relay 1490 Internet Engineering Task Force (IETF). To remove the DLCI-to-VCD connection, use the **no** form of this command.

```
fr-atm connect dlci dlci atm-interface [pvc name | [pvc vpi/vci] [clp-bit {map-de | 0 | 1}] [de-bit {no-map-clp | map-clp}]
```

```
no fr-atm connect dlci dlci atm-interface [pvc name | [pvc vpi/vci] [clp-bit {map-de | 0 | 1}] [de-bit {no-map-clp | map-clp}]
```

Syntax Description		
	<i>dlci</i>	Frame Relay DLCI number.
	<i>atm-interface</i>	The ATM interface connected to the DLCI.
	<b>pvc name</b>	(Optional) The ATM PVC name.
	<b>pvc vpi/vci</b>	(Optional) The ATM PVC virtual path identifier (VPI)/virtual channel identifier (VCI). The default value for <i>vpi</i> is 0 if no value is entered.  When specifying the ATM PVC, enter one of the following PVC designations: <ul style="list-style-type: none"> <li>• The <i>name</i> value</li> <li>• The <i>vpi</i> value alone</li> <li>• The <i>vpi/vci</i> combination</li> </ul>
	<b>clp-bit</b> { <b>map-de</b>   <b>0</b>   <b>1</b> }	(Optional) Sets the mode of Discard Eligibility/Cell Loss Priority (DE/CLP) mapping in the Frame Relay to ATM direction. The default is <b>map-de</b> .  <b>map-de</b> —Specifies Mode 1 (as described in section 4.4.2 of FRF.5). <b>0</b> or <b>1</b> —Specifies Mode 2 (as described in section 4.4.2 of FRF.5).
	<b>de-bit</b> { <b>no-map-clp</b>   <b>map-clp</b> }	(Optional) Sets the mode of DE/CLP mapping in the ATM to Frame Relay direction. The default is <b>map-clp</b> .  <b>map-clp</b> —Specifies Mode 1 (as described in section 4.4.2 of FRF.5). <b>no-map-clp</b> —Specifies Mode 2 (as described in section 4.4.2 of FRF.5).

## frame-relay adaptive-shaping

To select the type of backward notification you want to use, use the **frame-relay adaptive-shaping** map-class configuration command. To disable backward notification, use the **no** form of the command.

**frame-relay adaptive-shaping { becn | foresight }**

**no frame-relay adaptive-shaping**

Syntax Description	becn	foresight
	Enables rate adjustment in response to backward explicit congestion notification (BECN).	Enables rate adjustment in response to ForeSight messages.

## frame-relay address registration auto-address

To enable a router to automatically select a management IP address for ELMI address registration, use the **frame-relay address registration auto-address** global configuration command. To disable automatic address selection, use the **no** form of this command.

**frame-relay address registration auto-address**

**no frame-relay address registration auto-address**

Syntax Description	This command has no arguments or keywords.

## frame-relay address registration ip

To configure the IP address for ELMI address registration, use the **frame-relay address registration ip** global configuration command. To set the IP address to 0.0.0.0, use the **no** form of this command.

**frame-relay address registration ip *address***

**no frame-relay address registration ip**

Syntax Description	<i>address</i>	IP address to be used for ELMI address registration.

## frame-relay address-reg enable

To enable ELMI address registration on an interface, use the **frame-relay address-reg enable** interface configuration command. To disable ELMI address registration, use the **no** form of this command.

**frame-relay address-reg enable**

**no frame-relay address-reg enable**

**Syntax Description** This command has no arguments or keywords.

## frame-relay bc

To specify the incoming or outgoing committed burst size (Bc) for a Frame Relay virtual circuit, use the **frame-relay bc** map-class configuration command. To reset the committed burst size to the default, use the **no** form of this command.

**frame-relay bc** {in | out} *bits*

**no frame-relay bc** {in | out} *bits*

<b>Syntax Description</b>	<b>in   out</b>	Incoming or outgoing; if neither is specified, both in and out values are set.
	<i>bits</i>	Committed burst size, in bits.

## frame-relay be

To set the incoming or outgoing excess burst size (Be) for a Frame Relay virtual circuit, use the **frame-relay be** map-class configuration command. To reset the excess burst size to the default, use the **no** form of this command.

**frame-relay be** {in | out} *bits*

**no frame-relay be** {in | out} *bits*

<b>Syntax Description</b>	<b>in   out</b>	Incoming or outgoing.
	<i>bits</i>	Excess burst size, in bits.

## frame-relay becn-response-enable

This **frame-relay becn-response-enable** command has been replaced by the **frame-relay adaptive-shaping** command. See the description of the **frame-relay adaptive-shaping** command for more information.

## frame-relay broadcast-queue

To create a special queue for a specified interface to hold broadcast traffic that has been replicated for transmission on multiple data-link connection identifiers (DLCIs), use the **frame-relay broadcast-queue** interface configuration command.

```
frame-relay broadcast-queue size byte-rate packet-rate
```

Syntax Description		
	<i>size</i>	Number of packets to hold in the broadcast queue.
	<i>byte-rate</i>	Maximum number of bytes to be sent per second.
	<i>packet-rate</i>	Maximum number of packets to be sent per second.

## frame-relay cir

To specify the incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit, use the **frame-relay cir** map-class configuration command. To reset the CIR to the default, use the **no** form of this command.

```
frame-relay cir {in | out} bps
```

```
no frame-relay cir {in | out} bps
```

Syntax Description		
	<i>in   out</i>	Incoming or outgoing.
	<i>bps</i>	CIR in bits per second.

## frame-relay class

To associate a map class with an interface or subinterface, use the **frame-relay class** interface configuration command. To remove the association between the interface or subinterface and the named map class, use the **no** form of this command.

```
frame-relay class name
```

```
no frame-relay class name
```

Syntax Description		
	<i>name</i>	Name of the map class to associate with this interface or subinterface.

## frame-relay congestion-management

To enable Frame Relay congestion management functions on all switched permanent virtual circuits (PVCs) on an interface, and to enter Frame Relay congestion management configuration mode, use the **frame-relay congestion-management** interface configuration command. To disable Frame Relay congestion management, use the **no** form of this command.

**frame-relay congestion-management**

**no frame-relay congestion-management**

---

**Syntax Description** This command has no arguments or keywords.

## frame-relay congestion threshold de

To configure the threshold at which discard-eligible (DE)-marked packets will be discarded from the traffic-shaping queue of a switched permanent virtual circuit (PVC), use the **frame-relay congestion threshold de** map-class configuration command. To reconfigure the threshold, use the **no** form of this command.

**frame-relay congestion threshold de** *percentage*

**no frame-relay congestion threshold de** *percentage*

---

<b>Syntax Description</b>	<i>percentage</i>	Threshold at which DE-marked packets will be discarded, specified as a percentage of the maximum queue size.
---------------------------	-------------------	--

---

## frame-relay congestion threshold ecn

To configure the threshold at which explicit congestion notice (ECN) bits will be set on packets in the traffic-shaping queue of a switched permanent virtual circuit (PVC), use the **frame-relay congestion threshold ecn** map-class configuration command. To reconfigure the threshold, use the **no** form of this command.

**frame-relay congestion threshold ecn** *percentage*

**no frame-relay congestion threshold ecn** *percentage*

---

<b>Syntax Description</b>	<i>percentage</i>	Threshold at which ECN bits will be set on packets, specified as a percentage of the maximum queue size.
---------------------------	-------------------	--

---

## frame-relay custom-queue-list

To specify a custom queue to be used for the virtual circuit queueing associated with a specified map class, use the **frame-relay custom-queue-list** map-class configuration command. To remove the specified queueing from the virtual circuit and cause it to revert to the default first-come, first-served queueing, use the **no** form of this command.

**frame-relay custom-queue-list** *list-number*

**no frame-relay custom-queue-list** *list-number*

<b>Syntax Description</b>	<i>list-number</i> Custom queue list number.
---------------------------	--

## frame-relay de-group

To specify the discard eligibility (DE) group number to be used for a specified data-link connection identifier (DLCI), use the **frame-relay de-group** interface configuration command. To disable a previously defined group number assigned to a specified DLCI, use the **no** form of the command with the relevant keyword and arguments.

**frame-relay de-group** *group-number dlc*

**no frame-relay de-group** [*group-number*] [*dlci*]

<b>Syntax Description</b>	<i>group-number</i> DE group number to apply to the specified DLCI number, between 1 and 10.
	<i>dlci</i> DLCI number.

## frame-relay de-list

To define a discard eligibility (DE) list specifying the packets that have the DE bit set and thus are eligible for discarding when congestion is experienced on the Frame Relay switch, use the **frame-relay de-list** global configuration command. To delete a portion of a previously defined DE list, use the **no** form of this command.

**frame-relay de-list** *list-number* {**protocol** *protocol* | **interface** *type number*} *characteristic*

**no frame-relay de-list** *list-number* {**protocol** *protocol* | **interface** *type number*} *characteristic*

Syntax Description		
	<i>list-number</i>	Number of the DE list.
	<b>protocol</b> <i>protocol</i>	One of the following keywords corresponding to a supported protocol or device:  <b>arp</b> —Address Resolution Protocol <b>apollo</b> —Apollo Domain <b>appletalk</b> —AppleTalk <b>bridge</b> —bridging device <b>clns</b> —ISO Connectionless Network Service <b>clns_es</b> —CLNS end systems <b>clns_is</b> —CLNS intermediate systems. <b>compressedtcp</b> —Compressed Transmission Control Protocol (TCP) <b>decnet</b> —DECnet <b>decnet_node</b> —DECnet end node <b>decnet_router-L1</b> —DECnet Level 1 (intra-area) router <b>decnet_router-L2</b> —DECnet Level 2 (interarea) router <b>ip</b> —Internet Protocol <b>ipx</b> —Novell Internet Packet Exchange Protocol <b>vines</b> —Banyan VINES <b>xns</b> —Xerox Network Systems
	<b>interface type</b>	One of the following interface types: <b>serial</b> , <b>null</b> , or <b>ethernet</b> .
	<i>number</i>	Interface number.
	<i>characteristic</i>	One of the following:  <b>fragments</b> —Fragmented IP packets <b>gt bytes</b> —Sets the DE bit for packets larger than the specified number of bytes (including the 4 byte Frame Relay Encapsulation) <b>list access-list-number</b> —Previously defined access list number <b>lt bytes</b> —Sets the DE bit for packets smaller than the specified number of bytes (including the 4 byte Frame Relay Encapsulation) <b>tcp port</b> —TCP packets to or from a specified port <b>udp port</b> —User Datagram Protocol (UDP) packets to or from a specified port

## frame-relay end-to-end keepalive error-threshold

To modify the keepalive error threshold value, use the **frame-relay end-to-end keepalive error-threshold** map-class configuration command. To reset the error threshold value to its default, use the **no** form of this command.

```
frame-relay end-to-end keepalive error-threshold {send | receive} count
```

```
no frame-relay end-to-end keepalive error-threshold {send | receive}
```

Syntax Description		
	<b>send</b>	Number of send-side errors in the event window before keepalive status goes from up to down.
	<b>receive</b>	Number of receive-side errors in the event window before keepalive status goes from up to down.
	<i>count</i>	Number of errors required. The maximum value is 32.

## frame-relay end-to-end keepalive event-window

To modify the keepalive event window value, use the **frame-relay end-to-end keepalive event-window** map-class configuration command. To reset the default event window size, use the **no** form of this command.

```
frame-relay end-to-end keepalive event-window {send | receive} size
```

```
no frame-relay end-to-end keepalive event-window {send | receive}
```

### Syntax Description

<b>send</b>	The size of the send-side event window.
<b>receive</b>	The size of the receive-side event window.
<i>size</i>	Number of events in the event window. The maximum value is 32.

## frame-relay end-to-end keepalive mode

To enable Frame Relay end-to-end keepalives, use the **frame-relay end-to-end keepalive mode** map-class configuration command. To disable Frame Relay end-to-end keepalives, use the **no** form of this command.

```
frame-relay end-to-end keepalive mode {bidirectional | request | reply | passive-reply}
```

```
no frame-relay end-to-end keepalive mode
```

### Syntax Description

<b>bidirectional</b>	Enables bidirectional mode.
<b>request</b>	Enables request mode.
<b>reply</b>	Enables reply mode.
<b>passive-reply</b>	Enables passive reply mode.

## frame-relay end-to-end keepalive success-events

To modify the keepalive success events value, use the **frame-relay end-to-end keepalive success-events** map-class configuration command. To reset the success events value to its default, use the **no** form of this command.

```
frame-relay end-to-end keepalive success-events {send | receive} count
```

```
no frame-relay end-to-end keepalive success-events {send | receive}
```

### Syntax Description

<b>send</b>	The number of consecutive send-side success events required to change the keepalive state from down to up.
<b>receive</b>	The number of consecutive receive-side success events required to change the keepalive state from down to up.
<i>count</i>	Number of consecutive success events required. The maximum value is 32.

## frame-relay end-to-end keepalive timer

To modify the keepalive timer value, use the **frame-relay end-to-end keepalive timer** map-class configuration command. To reset the timer value to its default, use the **no** form of this command.

```
frame-relay end-to-end keepalive timer {send | receive} interval
```

```
no frame-relay end-to-end keepalive timer {send | receive}
```

Syntax Description	
<b>send</b>	How frequently to send a keepalive request.
<b>receive</b>	How long before the receive-side error counter is incremented if no request is received.
<i>interval</i>	Time in seconds for the timer to expire.

## frame-relay fair-queue

To enable weighted fair queueing for one or more Frame Relay permanent virtual circuits (PVCs), use the **frame-relay fair-queue** map-class configuration command in conjunction with the **map-class frame-relay** command. To disable weighted fair queueing for a Frame Relay map class, use the **no** form of this command.

```
frame-relay fair-queue [congestive_discard_threshold [number_dynamic_conversation_queues
[number_reservable_conversation_queues [max_buffer_size_for_fair_queues]]]]
```

```
no frame-relay fair-queue [congestive_discard_threshold
[number_dynamic_conversation_queues [number_reservable_conversation_queues
[max_buffer_size_for_fair_queues]]]]
```

Syntax Description	
<i>congestive_discard_threshold</i>	(Optional) Specifies the number of messages allowed in each queue. The range is from 1 to 4096 messages; the default is 64.
<i>number_dynamic_conversation_queues</i>	(Optional) Specifies the number of dynamic queues to be used for best-effort conversations—normal conversations not requiring any special network services. Valid values are 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096; the default is 16.
<i>number_reservable_conversation_queues</i>	(Optional) Specifies the number of reserved queues to be used for carrying voice traffic. The range is from 0 to 100; the default is 2. (The command line interface (CLI) will not allow a value less than 2 if fragmentation is configured on the frame relay map-class.)
<i>max_buffer_size_for_fair_queues</i>	(Optional) Specifies the maximum buffer size in bytes for all of the fair queues. The range is from 0 to 4096 bytes; the default is 600.

## frame-relay fragment

To enable fragmentation of Frame Relay frames for a Frame Relay map class, use the **frame-relay fragment** map-class configuration command. To disable Frame Relay fragmentation, use the **no** form of this command.

**frame-relay fragment** *fragment\_size* [**switched**]

**no frame-relay fragment**

<b>Syntax Description</b>	<i>fragment_size</i>	Specifies the number of payload bytes from the original Frame Relay frame that will go into each fragment. This number excludes the Frame Relay header of the original frame.  All the fragments of a Frame Relay frame except the last will have a payload size equal to <i>fragment_size</i> ; the last fragment will have a payload less than or equal to <i>fragment_size</i> . Valid values are from 16 to 1600 bytes; the default is 53.
	<b>switched</b>	(Optional) Specifies that fragmentation will be enabled on a switched permanent virtual circuit (PVC).

## frame-relay holdq

To configure the maximum size of a traffic-shaping queue on a switched PVC, use the **frame-relay holdq** map-class configuration command. To reconfigure the size of the queue, use the **no** form of this command.

**frame-relay holdq** *queue-size*

**no frame-relay holdq** *queue-size*

<b>Syntax Description</b>	<i>queue-size</i>	Size of the traffic-shaping queue, as specified in maximum number of packets. The range is from 1 to 512.
---------------------------	-------------------	---

## frame-relay idle-timer

To specify the idle timeout interval for a switched virtual circuit (SVC), use the **frame-relay idle-timer** map-class configuration command. To reset the idle timer to its default interval, use the **no** form of this command.

**frame-relay idle-timer** [**in** | **out**] *seconds*

**no frame-relay idle-timer** *seconds*

<b>Syntax Description</b>	<b>in</b>	(Optional) timeout interval applies to inbound packet activity.
	<b>out</b>	(Optional) timeout interval applies to outbound packet activity.
	<i>seconds</i>	Time interval, in seconds, with no frames exchanged on a switched virtual circuit, after which the SVC is released.

## frame-relay interface-dlci

To assign a data-link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server, or to assign a specific permanent virtual circuit (PVC) to a DLCI, or to apply a virtual template configuration for a PPP session, use the **frame-relay interface-dlci** interface configuration command. To remove this assignment, use the **no** form of this command.

```
frame-relay interface-dlci dlci [ietf | cisco] [voice-cir cir] [ppp virtual-template-name]
```

```
no frame-relay interface-dlci dlci [ietf | cisco] [voice-cir cir] [ppp virtual-template-name]
```

### BOOTP server only

```
frame-relay interface-dlci dlci [protocol ip ip-address]
```

<b>Syntax Description</b>	<i>dlci</i>	DLCI number to be used on the specified subinterface.
	<b>ietf</b>   <b>cisco</b>	(Optional) Encapsulation type: Internet Engineering Task Force (IETF) Frame Relay encapsulation or Cisco Frame Relay encapsulation.
	<b>voice-cir</b> <i>cir</i>	(Optional; supported on the Cisco MC3810 only.) Specifies the upper limit on the voice bandwidth that may be reserved for this DLCI. The default is the committed information rate (CIR) configured for the Frame Relay map class.
	<b>ppp</b>	(Optional) Enables the circuit to use the PPP in Frame Relay encapsulation.
	<i>virtual-template-name</i>	(Optional) Specifies which virtual template interface to apply the PPP connection to.
	<b>protocol ip</b> <i>ip-address</i>	(Optional) Indicates the IP address of the main interface of a new router or access server onto which a router configuration file is to be automatically installed over a Frame Relay network. Use this option only when this device will act as the BOOTP server for automatic installation over Frame Relay.

## frame-relay interface-dlci switched

To indicate that a Frame Relay data-link connection identifier (DLCI) is switched, use the **frame-relay interface-dlci switched** interface configuration command. To remove this assignment, use the **no** form of this command.

```
frame-relay interface-dlci dlci switched
```

```
no frame-relay interface-dlci dlci switched
```

Syntax Description	<i>dlci</i>	DLCI number to be used on the specified interface or subinterface.
--------------------	-------------	--

## frame-relay intf-type

To configure a Frame Relay switch type, use the **frame-relay intf-type** interface configuration command. To disable the switch, use the **no** form of this command.

```
frame-relay intf-type [dce | dte | nni]
```

```
no frame-relay intf-type [dce | dte | nni]
```

Syntax Description	<b>dce</b>	(Optional) Router or access server functions as a switch connected to a router.
	<b>dte</b>	(Optional) Router or access server is connected to a Frame Relay network.
	<b>nni</b>	(Optional) Router or access server functions as a switch connected to a switch—supports Network-to-Network Interface (NNI) connections.

## frame-relay inverse-arp

To reenabling Inverse Address Resolution Protocol (Inverse ARP) on a specified interface or subinterface if the Inverse ARP was previously disabled on a router or access server configured for Frame Relay, use the **frame-relay inverse-arp** interface configuration command. To disable this feature, use the **no** form of this command.

```
frame-relay inverse-arp [protocol] [dlci]
```

```
no frame-relay inverse-arp [protocol] [dlci]
```

Syntax Description	<i>protocol</i>	(Optional) Supported protocols: <b>appletalk</b> , <b>decnet</b> , <b>ip</b> , <b>ipx</b> , <b>vines</b> , and <b>xns</b> .
	<i>dlci</i>	(Optional) One of the DLCI numbers used on the interface. Acceptable numbers are integers in the range from 16 through 1007.

## frame-relay ip tcp compression-connections

To specify the maximum number of TCP header compression connections that can exist on a Frame Relay interface, use the **frame-relay ip tcp compression-connections** interface configuration command. To restore the default, use the **no** form of this command.

**frame-relay ip tcp compression-connections** *number*

**no frame-relay ip tcp compression-connections**

<b>Syntax Description</b>	<i>number</i>	Maximum number of TCP header compression connections. The range is from 3 to 256.
---------------------------	---------------	---

## frame-relay ip tcp header-compression

To configure an interface to ensure that the associated permanent virtual circuit (PVC) will always carry outgoing TCP/IP headers in compressed form, use the **frame-relay ip tcp header-compression** interface configuration command. To disable compression of TCP/IP packet headers on the interface, use the **no** form of this command.

**frame-relay ip tcp header-compression** [*passive*]

**no frame-relay ip tcp header-compression**

<b>Syntax Description</b>	<b>passive</b>	(Optional) Compresses the outgoing TCP/IP packet header only if an incoming packet had a compressed header.
---------------------------	----------------	---

## frame-relay lapf frmr

To resume the default setting of sending the Frame Reject (FRMR) frame at the Link Access Procedure for Frame Relay (LAPF) Frame Reject procedure after having set the option of not sending the frame, use the **frame-relay lapf frmr** command. To set the option of *not* sending the Frame Reject (FRMR) frame at the LAPF Frame Reject procedure, use the **no** form of this command.

**frame-relay lapf frmr**

**no frame-relay lapf frmr**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## frame-relay lapf k

To set the Link Access Procedure for Frame Relay (LAPF) window size *k*, use the **frame-relay lapf k** interface configuration command. To reset the maximum window size *k* to the default value, use the **no** form of this command.

**frame-relay lapf k** *number*

**no frame-relay lapf k** [*number*]

<b>Syntax Description</b>	<i>number</i>	Maximum number of Information frames that either are outstanding for transmission or are transmitted but unacknowledged, in the range from 1 through 127.
---------------------------	---------------	---

## frame-relay lapf n200

To set the Link Access Procedure for Frame Relay (LAPF) maximum retransmission count *N200*, use the **frame-relay lapf n200** interface configuration command. To reset the maximum retransmission count to the default of 3, use the **no** form of this command.

**frame-relay lapf n200** *retries*

**no frame-relay lapf n200** [*retries*]

<b>Syntax Description</b>	<i>retries</i>	Maximum number of retransmissions of a frame.
---------------------------	----------------	---

## frame-relay lapf n201

To set the Link Access Procedure for Frame Relay (LAPF) N201 value (the maximum length of the Information field of the LAPF I frame), use the **frame-relay lapf n201** interface configuration command. To reset the maximum length of the Information field to the default of 260 bytes (octets), use the **no** form of this command.

**frame-relay lapf n201** *bytes*

**no frame-relay lapf n201** [*bytes*]

<b>Syntax Description</b>	<i>bytes</i>	Maximum number of bytes in the Information field of the LAPF I frame, between 1 and 16384.
---------------------------	--------------	--

## frame-relay lapf t200

To set the Link Access Procedure for Frame Relay (LAPF) retransmission timer value T200, use the **frame-relay lapf t200** interface configuration command. To reset the T200 timer to the default value of 15, use the **no** form of this command.

**frame-relay lapf t200** *tenths-of-a-second*

**no frame-relay lapf t200**

<b>Syntax Description</b>	<i>tenths-of-a-second</i>	Time, in tenths of a second, in the range from 1 through 100.
---------------------------	---------------------------	---

## frame-relay lapf t203

To set the Link Access Procedure for Frame Relay (LAPF) link idle timer value T203 of data-link connection identifier (DLCI) 0, use the **frame-relay lapf t203** interface configuration command. To reset the link idle timer to the default value, use the **no** form of this command.

**frame-relay lapf t203** *seconds*

**no frame-relay lapf t203**

<b>Syntax Description</b>	<i>seconds</i>	Maximum time allowed with no frames exchanged, in the range from 1 through 65535 seconds.
---------------------------	----------------	---

## frame-relay lmi-n391dte

To set a full status polling interval, use the **frame-relay lmi-n391dte** interface configuration command. To restore the default interval value, assuming that a Local Management Interface (LMI) has been configured, use the **no** form of this command.

**frame-relay lmi-n391dte** *keep-exchanges*

**no frame-relay lmi-n391dte** *keep-exchanges*

<b>Syntax Description</b>	<i>keep-exchanges</i>	Number of keep exchanges to be done before requesting a full status message. Acceptable value is a positive integer in the range from 1 through 255.
---------------------------	-----------------------	--

## frame-relay lmi-n392dce

To set the data communications equipment (DCE) and the Network-to-Network Interface (NNI) error threshold, use the **frame-relay lmi-n392dce** interface configuration command. To remove the current setting, use the **no** form of this command.

**frame-relay lmi-n392dce** *threshold*

**no frame-relay lmi-n392dce** *threshold*

---

<b>Syntax Description</b>	<i>threshold</i>	Error threshold value. Acceptable value is a positive integer in the range from 1 through 10.
---------------------------	------------------	---

---

## frame-relay lmi-n392dte

To set the error threshold on a data terminal equipment (DTE) or network-to-network interface (NNI) interface, use the **frame-relay lmi-n392dte** interface configuration command. To remove the current setting, use the **no** form of this command.

**frame-relay lmi-n392dte** *threshold*

**no frame-relay lmi-n392dte** *threshold*

---

<b>Syntax Description</b>	<i>threshold</i>	Error threshold value. Acceptable value is a positive integer in the range from 1 through 10.
---------------------------	------------------	---

---

## frame-relay lmi-n393dce

To set the data communications equipment (DCE) and Network-to-Network Interface (NNI) monitored events count, use the **frame-relay lmi-n393dce** interface configuration command. To remove the current setting, use the **no** form of this command.

**frame-relay lmi-n393dce** *events*

**no frame-relay lmi-n393dce** *events*

---

<b>Syntax Description</b>	<i>events</i>	Value of monitored events count. Acceptable value is a positive integer in the range from 1 through 10.
---------------------------	---------------	---

---

## frame-relay lmi-n393dte

To set the monitored event count on a data terminal equipment (DTE) or Network-to-Network Interface (NNI) interface, use the **frame-relay lmi-n393dte** interface configuration command. To remove the current setting, use the **no** form of this command.

```
frame-relay lmi-n393dte events
```

```
no frame-relay lmi-n393dte events
```

<b>Syntax Description</b>	<i>events</i> Value of monitored events count. Acceptable value is a positive integer in the range from 1 through 10.
---------------------------	---

## frame-relay lmi-t392dce

To set the polling verification timer on a data communications equipment (DCE) or Network-to-Network Interface (NNI) interface, use the **frame-relay lmi-t392dce** interface configuration command. To remove the current setting, use the **no** form of this command.

```
frame-relay lmi-t392dce seconds
```

```
no frame-relay lmi-t392dce seconds
```

<b>Syntax Description</b>	<i>seconds</i> Polling verification timer value from 5 to 30 seconds.
---------------------------	---

## frame-relay lmi-type

To select the Local Management Interface (LMI) type, use the **frame-relay lmi-type** interface configuration command. To return to the default LMI type, use the **no** form of this command.

```
frame-relay lmi-type {ansi | cisco | q933a}
```

```
no frame-relay lmi-type {ansi | q933a}
```

<b>Syntax Description</b>	<b>ansi</b> Annex D defined by American National Standards Institute (ANSI) standard T1.617.
	<b>cisco</b> LMI type defined jointly by Cisco and three other companies.
	<b>q933a</b> ITU-T Q.933 Annex A.

## frame-relay local-dlci

To set the source data-link connection identifier (DLCI) for use when the Local Management Interface (LMI) is not supported, use the **frame-relay local-dlci** interface configuration command. To remove the DLCI number, use the **no** form of this command.

**frame-relay local-dlci** *number*

**no frame-relay local-dlci**

Syntax Description	<i>number</i>	Local (source) DLCI number to be used.
--------------------	---------------	--

## frame-relay map

To define the mapping between a destination protocol address and the data-link connection identifier (DLCI) used to connect to the destination address, use the **frame-relay map** interface configuration command. To delete the map entry, use the **no** form of this command.

**frame-relay map** *protocol protocol-address dlci* [**broadcast**] [**ietf** | **cisco**] [**payload-compress** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]

**no frame-relay map** *protocol protocol-address*

Syntax Description	<i>protocol</i>	Supported protocol, bridging, or logical link control keywords: <b>appletalk</b> , <b>decnet</b> , <b>dlsiw</b> , <b>ip</b> , <b>ipx</b> , <b>llc2</b> , <b>rsrb</b> , <b>vines</b> , and <b>xns</b> .
	<i>protocol-address</i>	Destination protocol address.
	<i>dlci</i>	DLCI number used to connect to the specified protocol address on the interface.
	<b>broadcast</b>	(Optional) Forwards broadcasts to this address when multicast is not enabled (see the <b>frame-relay multicast-dlci</b> command for more information about multicasts). This keyword also simplifies the configuration of Open Shortest Path First (OSPF).
	<b>ietf</b>	(Optional) Internet Engineering Task Force (IETF) form of Frame Relay encapsulation. Used when the router or access server is connected to the equipment of another vendor across a Frame Relay network.
	<b>cisco</b>	(Optional) Cisco encapsulation method.
	<b>payload-compress</b>	(Optional) Enables payload compression.
	<b>packet-by-packet</b>	(Optional) Packet-by-packet payload compression using the Stacker method.

<b>frf9 stac</b>	(Optional) FRF.9 compression using the Stacker method: <ul style="list-style-type: none"> <li>• If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression).</li> <li>• If the CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression).</li> <li>• If the second-generation Versatile Interface Processor (VIP2) is not available, compression is performed in the main processor of the router (software compression).</li> </ul>
<b>data-stream stac</b>	(Optional) Data-stream compression using the Stacker method: <ul style="list-style-type: none"> <li>• If the router contains a CSA, compression is performed in the CSA hardware (hardware compression).</li> <li>• If the CSA is not available, compression is performed in the main processor of the router (software compression).</li> </ul>
<i>hardware-options</i>	Choose one of the following hardware options: <ul style="list-style-type: none"> <li>• (Optional) <b>distributed</b>. Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression.</li> <li>• (Optional) <b>software</b>. Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router.</li> <li>• (Optional) <b>csa csa_number</b>. Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.</li> </ul>

## frame-relay map bridge

To specify that broadcasts are to be forwarded during bridging, use the **frame-relay map bridge** interface configuration command. To delete the map entry, use the **no** form of this command.

**frame-relay map bridge** *dcli* [**broadcast**] [**ietf**]

**no frame-relay map bridge** *dcli*

Syntax Description	
<i>dcli</i>	DLCI number to be used for bridging on the specified interface or subinterface.
<b>broadcast</b>	(Optional) Broadcasts are forwarded when multicast is not enabled.
<b>ietf</b>	(Optional) IETF form of Frame Relay encapsulation. Use when the router or access server is connected to another vendor's equipment across a Frame Relay network.

## frame-relay map clns

To forward broadcasts when Connectionless Network Service (CLNS) is used for routing, use the **frame-relay map clns** interface configuration command. To delete the map entry, use the **no** form of this interface configuration command.

```
frame-relay map clns dci [broadcast]
```

```
no frame-relay map clns dci
```

Syntax Description		
	<i>dci</i>	DLCI number to which CLNS broadcasts are forwarded on the specified interface.
	<b>broadcast</b>	(Optional) Broadcasts are forwarded when multicast is not enabled.

## frame-relay map ip tcp header-compression

To assign to an IP map header compression characteristics that differ from the compression characteristics of the interface with which the IP map is associated, use the **frame-relay map ip tcp header-compression** interface configuration command.

```
frame-relay map ip ip-address dci [broadcast] tcp header-compression [active | passive]  
[connections number]
```

Syntax Description		
	<i>ip-address</i>	IP address of the destination or next hop.
	<i>dci</i>	Data-link connection identifier (DLCI) number.
	<b>broadcast</b>	(Optional) Forwards broadcasts to the specified IP address.
	<b>active</b>	(Optional) Compresses the header of every outgoing TCP/IP packet.
	<b>passive</b>	(Optional) Compresses the header of an outgoing TCP/IP packet only if an incoming TCP/IP packet had a compressed header.
	<b>connections</b> <i>number</i>	(Optional) Specifies the maximum number of TCP header compression connections. The range is from 3 to 256.

## frame-relay mincir

To specify the minimum acceptable incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit, use the **frame-relay mincir** map-class configuration command. To reset the minimum acceptable CIR to the default, use the **no** form of this command.

```
frame-relay mincir {in | out} bps
```

```
no frame-relay mincir
```

Syntax Description	in   out	Incoming or outgoing.
	<i>bps</i>	Committed information rate, in bits per second.

## frame-relay multicast-dlci

To define the data-link connection identifier (DLCI) to be used for multicasts, use the **frame-relay multicast-dlci** interface configuration command. To remove the multicast group, use the **no** form of this command.

```
frame-relay multicast-dlci number
```

```
no frame-relay multicast-dlci
```

Syntax Description	<i>number</i>	Multicast DLCI.
--------------------	---------------	-----------------

## frame-relay payload-compress

To enable Stacker payload compression on a specified point-to-point interface or subinterface, use the **frame-relay payload-compress** interface configuration command. To disable payload compression on a specified point-to-point interface or subinterface, use the **no** form of this command.

```
frame-relay payload-compress { packet-by-packet | frf9 stac [hardware-options] | data-stream stac [hardware-options] }
```

```
no frame-relay payload-compress { packet-by-packet | frf9 stac | data-stream stac }
```

Syntax Description	<b>packet-by-packet</b>	Packet-by-packet payload compression using the Stacker method.
	<b>frf9 stac</b>	Enables FRF.9 compression using the Stacker method. <ul style="list-style-type: none"> <li>• If the router contains a CSA<sup>1</sup>, compression is performed in the CSA hardware (hardware compression).</li> <li>• If the CSA is not available, compression is performed in the software installed on the VIP2<sup>2</sup> (distributed compression).</li> <li>• If the VIP2 is not available, compression is performed in the main processor of the router (software compression).</li> </ul>

<i>hardware-options</i>	<p>Choose one of the following hardware options:</p> <ul style="list-style-type: none"> <li>(Optional) <b>distributed</b>. Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression.</li> <li>(Optional) <b>software</b>. Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router.</li> <li>(Optional) <b>csa csa_number</b>. Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.</li> </ul>
<b>data-stream stac</b>	<p>Enables data-stream compression using the Stacker method.</p> <ul style="list-style-type: none"> <li>If the router contains a CSA, compression is performed in the CSA hardware (hardware compression).</li> <li>If the CSA is not available, compression is performed in the main processor of the router (software compression).</li> </ul>

1. CSA = compression service adapter
2. VIP2 = second-generation Versatile Interface Processor

## frame-relay policing

To enable Frame Relay policing on all switched PVCs on the interface, use the **frame-relay policing** interface configuration command. To disable Frame Relay policing, use the **no** form of this command.

**frame-relay policing**

**no frame-relay policing**

**Syntax Description** This command has no arguments or keywords.

## frame-relay priority-dlci-group

To prioritize multiple data-link connection identifiers (DLCIs) according to the type of Frame Relay traffic, use the **frame-relay priority-dlci-group** interface configuration command.

**frame-relay priority-dlci-group** *group-number high-dlci medium-dlci normal-dlci low-dlci*

<b>Syntax Description</b>	<i>group-number</i>	Specific group number.
	<i>high-dlci</i>	DLCI that is to have highest priority level.
	<i>medium-dlci</i>	DLCI that is to have medium priority level.

<i>normal-dlci</i>	DLCI that is to have normal priority level.
<i>low-dlci</i>	DLCI that is to have lowest priority level.

## frame-relay priority-group

To assign a priority queue to virtual circuits associated with a map class, use the **frame-relay priority-group** map-class configuration command. To remove the specified queueing from the virtual circuit and cause it to revert to the default first-come, first-served queueing, use the **no** form of this command.

**frame-relay priority-group** *list-number*

**no frame-relay priority-group** *list-number*

<b>Syntax Description</b>	<i>list-number</i>	Priority-list number to be associated with the specified map class.
---------------------------	--------------------	---

## frame-relay pvc

To configure Frame Relay permanent virtual circuits (PVCs) for FRF.8 Frame Relay-ATM Service Interworking, use the **frame-relay pvc** interface configuration command. To remove the PVC, use the **no** form of the command.

**frame-relay pvc** *dlci* **service** {**transparent** | **translation**} [**clp-bit** {**0** | **1** | **map-de**}] [**de-bit** {**0** | **1** | **map-clp**}] [**efci-bit** {**0** | **1** | **map-fecn**}] **interface atm0** {*vpi/vci* | *vcd*}

**no frame-relay pvc** *dlci* **service** {**transparent** | **translation**} [**clp-bit** {**0** | **1** | **map-de**}] [**de-bit** {**0** | **1** | **map-clp**}] [**efci-bit** {**0** | **1** | **map-fecn**}] **interface atm0** {*vpi/vci* | *vcd*}

<b>Syntax Description</b>	<i>dlci</i>	A value ranging from 16 to 1007 for the PVC's data-link connection identifier (DLCI). Use this label when you associate a Frame Relay PVC with an ATM PVC.
	<b>service</b> { <b>transparent</b>   <b>translation</b> }	In the <b>transparent</b> mode of Service Interworking, encapsulations are sent unaltered. In <b>translation</b> mode, mapping and translation take place. There is no default.
	<b>clp-bit</b> { <b>0</b>   <b>1</b>   <b>map-de</b> }	(Optional) Sets the mode of DE/CLP mapping in Frame Relay to the ATM direction. The default is <b>map-de</b> . <ul style="list-style-type: none"> <li><b>map-de</b>—Specifies Mode 1 (see section 4.2.1 of FRF.8)</li> <li><b>0</b> or <b>1</b>—Specifies Mode 2 (see section 4.2.1 of FRF.8)</li> </ul>
	<b>de-bit</b> { <b>0</b>   <b>1</b>   <b>map-clp</b> }	(Optional) Sets the mode of DE/CLP mapping in the ATM-to-Frame Relay direction. The default is <b>map-clp</b> . <ul style="list-style-type: none"> <li><b>map-clp</b>—Specifies Mode 1 (see section 4.2.1 of FRF.8)</li> <li><b>0</b> or <b>1</b>—Specifies Mode 2 (see section 4.2.1 of FRF.8)</li> </ul>

<b>efci-bit</b> { <b>0</b>   <b>1</b>   <b>map-fecn</b> }	(Optional) Sets FECN and the ATM EFCI in the Frame Relay-to-ATM direction. <b>map-fecn</b> is the default. <ul style="list-style-type: none"> <li><b>0</b>—Sets a constant value rather than mapping.</li> <li><b>1</b>—Sets a constant value rather than mapping.</li> <li><b>map-fecn</b>—Adheres to Mode 1 and maps the FECN indicators to EFCI indicators.</li> </ul>
<b>interface atm0</b> { <i>vpi/vci</i>   <i>vcd</i> }	Maps the Frame Relay PVC to an ATM PVC specified by slot number (0 is the only option for ATM on the Cisco MC3810) and either one of the following labels: <ul style="list-style-type: none"> <li><i>vpi/vci</i>—The virtual path identifier-virtual channel identifier (VPI-VCI) pair for the ATM PVC</li> <li><i>vcd</i>—The ATM virtual circuit descriptor (VCD) for the ATM PVC</li> </ul>

## frame-relay qos-autosense

To enable Enhanced Local Management Interface on the Cisco router, use the **frame-relay qos-autosense** interface configuration command. To disable Enhanced Local Management Interface on the Cisco router, use the **no** form of this command.

**frame-relay qos-autosense**

**no frame-relay qos-autosense**

**Syntax Description** This command has no arguments or keywords.

## frame-relay route

To specify the static route for permanent virtual circuit (PVC) switching, use the **frame-relay route** interface configuration command. To remove a static route, use the **no** form of this command.

**frame-relay route** *in-dlci* *out-interface* *out-dlci* [**voice-encap** *size*]

**no frame-relay route** *in-dlci* *out-interface* *out-dlci* [**voice-encap** *size*]

<b>Syntax Description</b>	<i>in-dlci</i>	DLCI on which the packet is received on the interface.
	<i>out-interface</i>	Interface that the router or access server uses to transmit the packet.
	<i>out-dlci</i>	DLCI that the router or access server uses to transmit the packet over the interface specified by the <i>out-interface</i> argument.
	<b>voice encap</b> <i>size</i>	(Optional) (Supported on the Cisco MC3810 only.) Specifies that data segmentation will be used to support Voice over Frame Relay. Note that the voice encapsulation applies only to the input DLCI side. The valid range is from 8 to 1600.

## frame-relay svc

To enable Frame Relay switched virtual circuit (SVC) operation on the specified interface, use the **frame-relay svc** interface configuration command. To disable SVC operation on the specified interface, use the **no** form of this command.

**frame-relay svc**

**no frame-relay svc**

---

**Syntax Description** This command has no arguments or keywords.

## frame-relay switching

To enable permanent virtual switching (PVC) switching on a Frame Relay DCE device or a Network-to-Network Interface (NNI), use the **frame-relay switching** global configuration command. To disable switching, use the **no** form of this command.

**frame-relay switching**

**no frame-relay switching**

---

**Syntax Description** This command has no arguments or keywords.

## frame-relay tc

To set the measurement interval for policing incoming traffic when the committed information rate (CIR) is zero, use the **frame-relay tc** map-class configuration command. To reset the measurement interval for policing, use the **no** form of this command.

**frame-relay tc** *milliseconds*

**no frame-relay tc** *milliseconds*

---

**Syntax Description** *milliseconds* Time interval from 10 ms to 10,000 ms, during which incoming traffic cannot exceed committed burst size (Bc) plus excess burst size (Be).

---

## frame-relay traffic-rate

To configure all the traffic shaping characteristics of a virtual circuit in a single command, use the **frame-relay traffic-rate** map-class configuration command. To remove the specified traffic shaping from the map class, use the **no** form of this command.

**frame-relay traffic-rate** *average* [*peak*]

**no frame-relay traffic-rate** *average* [*peak*]

<b>Syntax Description</b>	<i>average</i>	Average rate, in bits per second; equivalent to specifying the contracted committed information rate (CIR).
	<i>peak</i>	(Optional) Peak rate, in bits per second; equivalent to $CIR + Be/Tc = CIR (1 + Be/Bc) = CIR + EIR$ .

## frame-relay traffic-shaping

To enable both traffic shaping and per-virtual circuit queuing for all permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) on a Frame Relay interface, use the **frame-relay traffic-shaping** interface configuration command. To disable traffic shaping and per-virtual circuit queuing, use the **no** form of this command.

**frame-relay traffic-shaping**

**no frame-relay traffic-shaping**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## interface fr-atm

To create a Frame Relay-ATM Interworking interface on the Cisco MC3810 and to enter Frame Relay-ATM Interworking configuration mode, use the **interface fr-atm** global configuration command. To delete the Frame Relay-ATM Interworking interface, use the **no** form of this command.

**interface fr-atm** *number*

**no interface fr-atm** *number*

<b>Syntax Description</b>	<i>number</i>	The Frame Relay-ATM Interworking interface number. Valid range is from 0 to 20.
---------------------------	---------------	---

## keepalive (LMI)

To enable the Local Management Interface (LMI) mechanism for serial lines using Frame Relay encapsulation, use the **keepalive** interface configuration command. To disable this capability, use the **no** form of this command.

**keepalive** *number*

**no keepalive**

<b>Syntax Description</b>	<i>number</i>	Number of seconds that defines the keepalive interval. The interval must be set as a positive integer that is less than the interval set on the switch; see the <b>frame-relay lmi-t392dce</b> command description earlier in this chapter.
---------------------------	---------------	---

## map-class frame-relay

To specify a map class to define quality of service (QoS) values for a switched virtual circuit (SVC), use the **map-class frame-relay** global configuration command.

**map-class frame-relay** *map-class-name*

<b>Syntax Description</b>	<i>map-class-name</i>	Name of this map class.
---------------------------	-----------------------	-------------------------

## map-group

To associate a map list with a specific interface, use the **map-group** interface configuration command.

**map-group** *group-name*

<b>Syntax Description</b>	<i>group-name</i>	Name used in a <b>map-list</b> command.
---------------------------	-------------------	---

## map-list

To specify a map group and link it to a local E.164 or X.121 source address and a remote E.164 or X.121 destination address for Frame Relay switched virtual circuits (SVCs), use the **map-list** global configuration command. To delete a previous map-group link, use the **no** form of this command.

**map-list** *map-group-name* **source-addr** {**e164** | **x121**} *source-address* **dest-addr** {**e164** | **x121**}  
*destination-address*

**no map-list** *map-group-name* **source-addr** {**e164** | **x121**} *source-address* **dest-addr** {**e164** | **x121**}  
*destination-address*

<b>Syntax Description</b>	<i>map-group-name</i>	Name of the map group. This map group must be associated with a physical interface.
	<b>source-addr { e164   x121 }</b>	Type of source address.
	<i>source-address</i>	Address of the type specified (E.164 or X.121).
	<b>dest-addr { e164   x121 }</b>	Type of destination address.
	<i>destination-address</i>	Address of the type specified (E.164 or X.121).

## show frame-relay end-to-end keepalive

To display statistics about Frame Relay end-to-end keepalive, use the **show frame-relay end-to-end keepalive** EXEC command.

```
show frame-relay end-to-end keepalive [interface [DLCI]]
```

<b>Syntax Description</b>	<i>interface</i>	(Optional) Interface to display.
	<i>DLCI</i>	(Optional) DLCI to display.

## show frame-relay fragment

To display information about the Frame Relay fragmentation, use the **show frame-relay fragment** command in privileged EXEC mode.

```
show frame-relay fragment [interface interface [DLCI]]
```

<b>Syntax Description</b>	<b>interface</b>	(Optional) Indicates a specific interface for which Frame Relay fragmentation information will be displayed.
	<i>interface</i>	(Optional) Interface number containing the DLCI(s) for which you wish to display fragmentation information.
	<i>DLCI</i>	(Optional) Specific DLCI for which you wish to display fragmentation information.

## show frame-relay ip tcp header-compression

To display statistics and TCP/IP header compression information for the interface, use the **show frame-relay ip tcp header-compression** EXEC command.

```
show frame-relay ip tcp header-compression
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## show frame-relay lapf

To display information about the status of the internals of Frame Relay Layer 2 (LAPF) if switched virtual circuits (SVCs) are configured, use the **show frame-relay lapf** EXEC command.

```
show frame-relay lapf
```

---

**Syntax Description** This command has no arguments or keywords.

## show frame-relay lmi

To display statistics about the Local Management Interface (LMI), use the **show frame-relay lmi** EXEC command.

```
show frame-relay lmi [type number]
```

---

<b>Syntax Description</b>	<i>type</i>	(Optional) Interface type; it must be serial.
	<i>number</i>	(Optional) Interface number.

---

## show frame-relay map

To display the current map entries and information about the connections, use the **show frame-relay map** EXEC command.

```
show frame-relay map
```

---

**Syntax Description** This command has no arguments or keywords.

## show frame-relay pvc

To display statistics about permanent virtual circuits (PVCs) for Frame Relay interfaces, use the **show frame-relay pvc** privileged EXEC command.

```
show frame-relay pvc [interface interface][dlci]
```

---

<b>Syntax Description</b>	<b>interface</b>	(Optional) Indicates a specific interface for which PVC information will be displayed.
	<i>interface</i>	(Optional) Interface number containing the data-link connection identifiers (DLCIs) for which you wish to display PVC information.
	<i>dlci</i>	(Optional) A specific DLCI number used on the interface. Statistics for the specified PVC are displayed when a DLCI is also specified.

---

## show frame-relay qos-autosense

To display the quality of service (QoS) values sensed from the switch, use the **show frame-relay qos-autosense** EXEC command.

```
show frame-relay qos-autosense [interface number]
```

<b>Syntax Description</b>	<b>interface <i>number</i></b>	(Optional) Indicates the number of the physical interface for which you want to display QoS information.
---------------------------	--------------------------------	--

## show frame-relay route

To display all configured Frame Relay routes, along with their status, use the **show frame-relay route** EXEC command.

```
show frame-relay route
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## show frame-relay svc maplist

To display all the switched virtual circuits (SVCs) under a specified map list, use the **show frame-relay svc maplist** EXEC command.

```
show frame-relay svc maplist name
```

<b>Syntax Description</b>	<b><i>name</i></b>	Name of the map list.
---------------------------	--------------------	-----------------------

## show frame-relay traffic

To display the global Frame Relay statistics since the last reload, use the **show frame-relay traffic** EXEC command.

```
show frame-relay traffic
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## show running map-class

To display information about all or specific map classes configured on the router, use the **show running map-class** EXEC command.

```
show running map-class [atm | frame-relay | dialer] [name]
```

Syntax Description		
	<b>atm</b>	(Optional) ATM map classes.
	<b>frame-relay</b>	(Optional) Frame Relay map classes.
	<b>dialer</b>	(Optional) Dialer map classes.
	<i>name</i>	(Optional) Name of a specific map class.

## threshold de

To configure the threshold at which discard eligible (DE)-marked packets will be discarded from switched permanent virtual circuits (PVCs) on the output interface, use the **threshold de** Frame Relay congestion management configuration command. To remove the threshold configuration, use the **no** form of this command.

```
threshold de percentage
```

```
no threshold de percentage
```

Syntax Description		
	<i>percentage</i>	Threshold at which DE-marked packets will be discarded, specified as a percentage of maximum queue size.

## threshold ecn

To configure the threshold at which ECN bits will be set on packets in switched PVCs on the output interface, use the **threshold ecn** Frame Relay congestion management configuration command. To remove the threshold configuration, use the **no** form of this command.

```
threshold ecn {bc | be} percentage
```

```
no threshold ecn {bc | be} percentage
```

Syntax Description		
	<b>bc</b>	Specifies threshold for committed traffic.
	<b>be</b>	Specifies threshold for excess traffic.
	<i>percentage</i>	Threshold at which ECN bits will be set on packets, specified as a percentage of maximum queue size.

■ threshold ecn



## Frame Relay-ATM Interworking Commands

This chapter describes the function and syntax of the commands used to configure FRF.5 Frame Relay-ATM Network Interworking and FRF.8 Frame Relay-ATM Service Interworking. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Wide-Area Networking Command Reference*.

### clp-bit

To set the ATM cell loss priority (CLP) field in the ATM cell header, use the **clp-bit** connect submenu command. To disable ATM CLP bit mapping, use the **no** form of this command.

```
clp-bit {0 | 1 | map-de}
```

```
no clp-bit {0 | 1 | map-de}
```

Syntax Description		
	<b>0</b>	The CLP field in the ATM cell header is always set to 0.
	<b>1</b>	The CLP field in the ATM cell header is always set to 1.
	<b>map-de</b>	The discard eligible (DE) field in the Frame Relay header is mapped to the CLP field in the ATM cell header.

### connect (FRF.5)

To configure an FRF.5 one-to-one connection between two Frame Relay end users over an intermediate ATM network, or an FRF.5 many-to-one connection between two Frame Relay end users over an intermediate ATM network, use the **connect** global configuration command. To remove a connection, use the **no** form of this command.

```
connect connection-name {vc-group group-name | FR-interface FR-DLCI} ATM-interface  
ATM-VPI/VCI network-interworking
```

```
no connect connection-name {vc-group group-name | FR-interface FR-DLCI} ATM-interface  
ATM-VPI/VCI network-interworking
```

Syntax Description		
	<i>connection-name</i>	Specifies a connection name. Enter as a 15-character maximum string.
	<b>vc-group</b> <i>group-name</i>	Specifies a VC group name for a many-to-one FRF.5 connection. Enter as an 11-character maximum string.
	<i>FR-interface</i>	Specifies the Frame Relay interface type and number, for example, <b>serial1/0</b> .
	<i>FR-DLCI</i>	Specifies the Frame Relay data-link connection identifier (DLCI) in the range from 16 to 1007.
	<i>ATM-interface</i>	Specifies the ATM interface type and number, for example, <b>atm1/0</b> .
	<i>ATM-VPI/VCI</i>	Specifies the ATM virtual path identifier/virtual channel identifier (VPI/VCI). If a VPI is not specified, the default VPI is 0.
	<b>network-interworking</b>	Specifies FRF.5 network interworking. Not a valid keyword if the <b>vc-group</b> keyword is specified.

## connect (FRF.8)

To configure an FRF.8 one-to-one mapping between a Frame Relay data-link connection identifier (DLCI) and an ATM permanent virtual circuit (PVC), use the **connect** global configuration command. To remove a connection, use the **no** form of this command.

**connect** *connection-name FR-interface FR-DLCI ATM-interface ATM-VPI/VCI*  
**service-interworking**

**no connect** *connection-name FR-interface FR-DLCI ATM-interface ATM-VPI/VCI*  
**service-interworking**

Syntax Description		
	<i>connection-name</i>	Specifies a connection name. Enter as a 15-character maximum string.
	<i>FR-interface</i>	Specifies the Frame Relay interface type and number, for example, <b>serial1/0</b> .
	<i>FR-DLCI</i>	Specifies the Frame Relay data-link connection identifier (DLCI) in the range 16 to 1007.
	<i>ATM-interface</i>	Specifies the ATM interface type and number, for example <b>atm1/0</b> .
	<i>ATM-VPI/VCI</i>	Specifies the ATM virtual path identifier/virtual channel identifier (VPI/VCI). If a VPI is not specified, the default VPI is 0.
	<b>service-interworking</b>	Specifies FRF.8 service interworking.

## de-bit

To set the Frame Relay discard eligible (DE) bit field in the Frame Relay cell header for FRF.8 service interworking, use the **de-bit** connect submode command. To disable or reset Frame Relay DE bit mapping, use the **no** form of this command.

**de-bit** {0 | 1 | map-clp}

**no de-bit** {0 | 1 | map-clp}

<b>Syntax Description</b>	<b>0</b>	The DE field in the Frame Relay header is always set to 0.
	<b>1</b>	The DE field in the Frame Relay header is always set to 1.
	<b>map-clp</b>	The DE field is set to 1 when one or more cells belonging to a frame has its cell loss priority (CLP) field set.

## de-bit map-clp

To set Frame Relay discard eligible (DE) bit mapping for FRF.5 network interworking, use the **de-bit map-clp** connect submode command. To disable or reset Frame Relay DE bit mapping, use the **no** form of this command.

**de-bit map-clp**

**no de-bit map-clp**

**Syntax Description** This command has no arguments or keywords.

## efci-bit

To set the explicit forward congestion indication (EFCI) bit field in the ATM cell header for FRF.8 service interworking, use the **efci-bit** connect submode command. To disable or reset this bit, use the **no** form of this command.

**efci-bit {0 | map-fecn}**

**no efci-bit {0 | map-fecn}**

<b>Syntax Description</b>	<b>0</b>	The EFCI field in the ATM cell header is set to 0.
	<b>map-fecn</b>	The EFCI field in the ATM cell header is set to 1 when the forward explicit congestion notification (FECN) field in the Frame Relay header is set.

## service translation

To enable upper layer user protocol encapsulation for Frame Relay-to-ATM Service Interworking (FRF.8) feature, which allows mapping between encapsulated ATM protocol data units (PDUs) and encapsulated Frame Relay PDUs, use the **service translation** command in FRF.8 connection mode. To disable upper layer user protocol encapsulation, use the **no** form of this command.

**service translation**

**no service translation**

**Syntax Description** This command has no arguments or keywords.

## show vc-group

To display the names of all virtual circuit (VC) groups, use the **show vc-group** EXEC command.

```
show vc-group [group-name]
```

---

### Syntax Description

<i>group-name</i>	(Optional) Name defined by the <b>vc-group</b> command. If this argument is not specified, the names of all VC groups in the system are displayed.
-------------------	--

---

## shutdown (FR-ATM)

To shut down a Frame Relay-ATM Network Interworking (FRF.5) connection or a Frame Relay-ATM Service Interworking (FRF.8) connection, use the **shutdown** connect submode command. To disable disconnection, use the **no** form of this command.

```
shutdown
```

```
no shutdown
```

---

### Syntax Description

This command has no arguments or keywords.

## vc-group

To assign multiple Frame Relay data-link connection identifiers (DLCIs) to a virtual circuit (VC) group for Frame Relay-to-ATM Network Interworking (FRF.5), use the **vc-group** global configuration mode command. To disable the VC group assignments, use the **no** form of this command.

```
vc-group group-name
```

```
no vc-group group-name
```

The **vc-group** command requires the use of the following command in VC-group configuration mode to provide a map between Frame Relay DLCIs and Frame Relay-SSCS DLCIs:

```
FR-interface-name FR-DLCI [FR-SSCS-DLCI]
```

---

### Syntax Description

<i>group-name</i>	A VC group name entered as an 11-character maximum string.
-------------------	--

---

The following syntax description applies to the VC-group entries:

<i>FR-interface-name</i>	Frame Relay interface; for example, <b>serial0/0</b> .
<i>FR-DLCI</i>	Frame Relay DLCI number in the range 16 to 1007.
<i>FR-SSCS-DLCI</i>	(Optional) Frame Relay SSSS DLCI number in the range of 16 to 991. Default is 1022.

---



## SMDS Commands

---

This chapter describes the function and syntax of the SMDS commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Wide-Area Networking Command Reference*.

### arp

To enable Address Resolution Protocol (ARP) entries for static routing over the Switched Multimegabit Data Service (SMDS) network, use the following variation of the **arp** global configuration command. To disable this capability, use the **no** form of this command.

```
arp ip-address smds-address smds
```

```
no arp ip-address smds-address smds
```

Syntax Description		
	<i>ip-address</i>	IP address of the remote router.
	<i>smds-address</i>	12-digit SMDS address in the dotted notation <i>nnnn.nnnn.nnnn</i> (48 bits long).
	<b>smds</b>	Enables ARP for SMDS.

### encapsulation smds

To enable Switched Multimegabit Data Service (SMDS) on the desired interface, use the **encapsulation smds** interface configuration command.

```
encapsulation smds
```

Syntax Description	
	This command has no arguments or keywords.

## interface serial multipoint

To define a logical subinterface on a serial interface to support multiple logical IP subnetworks over Switched Multimegabit Data Service (SMDS), use the **interface serial multipoint** interface configuration command.

```
interface serial {interface | slot/port}.subinterface multipoint
```

Syntax	Description
<i>interface</i>	Interface number.
<i>slot/port</i>	Slot and port number related to specified subinterface (for Cisco 7000 and 7500 series routers).
<i>.subinterface</i>	Number for this subinterface; values in the range 0 to 255.

## show smds addresses

To display the individual addresses and the interface they are associated with, use the **show smds addresses** privileged EXEC command.

```
show smds addresses
```

**Syntax Description** This command has no arguments or keywords.

## show smds map

To display all Switched Multimegabit Data Service (SMDS) addresses that are mapped to higher-level protocol addresses, use the **show smds map** privileged EXEC command.

```
show smds map
```

**Syntax Description** This command has no arguments or keywords.

## show smds traffic

To display statistics about Switched Multimegabit Data Service (SMDS) packets the router has received, use the **show smds traffic** privileged EXEC command.

```
show smds traffic
```

**Syntax Description** This command has no arguments or keywords.

## smds address

To specify the Switched Multimegabit Data Service (SMDS) individual address for a particular interface, use the **smds address** interface configuration command. To remove the address from the configuration file, use the **no** form of this command.

**smds address** *smds-address*

**no smds address** *smds-address*

---

**Syntax Description**

*smds-address* Individual address provided by the SMDS service provider. It is protocol independent.

---

## smds dxi

To enable the Data Exchange Interface (DXI) version 3.2 support, use the **smds dxi** interface configuration command. To disable the DXI 3.2 support, use the **no** form of this command.

**smds dxi**

**no smds dxi**

---

**Syntax Description**

This command has no arguments or keywords.

## smds enable-arp

To enable dynamic Address Resolution Protocol (ARP), use the **smds enable-arp** interface configuration command. The multicast address for ARP must be set before this command is issued. To disable the interface once ARP has been enabled, use the **no** form of this command.

**smds enable-arp**

**no smds enable-arp**

---

**Syntax Description**

This command has no arguments or keywords.

## smds glean

To enable dynamic address mapping for Internet Packet Exchange (IPX) over Switched Multimegabit Data Service (SMDS), use the **smds glean** interface configuration command. To disable dynamic address mapping for IPX over SMDS, use the **no** form of this command.

**smds glean** *protocol* [*timeout-value*] [**broadcast**]

**no smds glean** *protocol*

Syntax Description		
	<i>protocol</i>	Protocol type. Only IPX is supported.
	<i>timeout-value</i>	(Optional) Time to live (TTL) value. Value can be from 1 to 65535 minutes. The default is 5 minutes. This value indicates how long a gleaned dynamic map is stored in the SMDS map table.
	<b>broadcast</b>	(Optional) Marks the gleaned protocol address as a candidate for broadcast packets. All broadcast requests are sent to the unicast SMDS address.

## smds multicast

To assign a multicast Switched Multimegabit Data Service (SMDS) E.164 address to a higher-level protocol, use the **smds multicast** interface configuration command. To remove an assigned multicast address, use the **no** form of this command with the appropriate address.

**smds multicast** *protocol smds-address*

**no smds multicast** *protocol smds-address*

Syntax Description		
	<i>protocol</i>	Protocol type.
	<i>smds-address</i>	SMDS address. Because SMDS does not incorporate broadcast addressing, a group address for a particular protocol must be defined to serve the broadcast function.

## smds multicast arp

To map the Switched Multimegabit Data Service (SMDS) address to a multicast address, use the **smds multicast arp** interface configuration command. To disable this feature, use the **no** form of this command.

**smds multicast arp** *smds-address* [*ip-address mask*]

**no smds multicast arp** *smds-address* [*ip-address mask*]

Syntax Description		
	<i>smds-address</i>	SMDS address in E.164 format.
	<i>ip-address</i>	(Optional) IP address.
	<i>mask</i>	(Optional) Subnet mask for the IP address.

## smds multicast bridge

To enable spanning-tree updates, use the **smds multicast bridge** interface configuration command. To disable this function, use the **no** form of this command.

**smds multicast bridge** *smds-address*

**no smds multicast bridge** *smds-address*

<b>Syntax Description</b>	<i>smds-address</i>	SMDS multicast address in E.164 format.
---------------------------	---------------------	---

## smds multicast ip

To map a Switched Multimegabit Data Service (SMDS) group address to a secondary IP address, use the **smds multicast ip** interface configuration command. To remove the address map, use the **no** form of this command.

**smds multicast ip** *smds-address* [*ip-address mask*]

**no smds multicast ip** *smds-address* [*ip-address mask*]

<b>Syntax Description</b>	<i>smds-address</i>	SMDS address in E.164 format.
	<i>ip-address</i>	(Optional) IP address.
	<i>mask</i>	(Optional) Subnet mask for the IP address.

## smds static-map

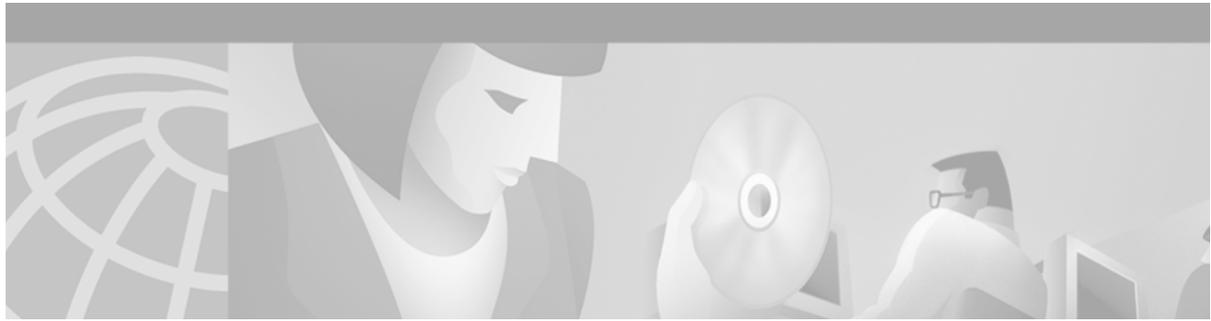
To configure a static map between an individual Switched Multimegabit Data Service (SMDS) address and a higher-level protocol address, use the **smds static-map** interface configuration command. To remove the map, use the **no** form of this command with the appropriate arguments.

**smds static-map** *protocol protocol-address smds-address* [**broadcast**]

**no smds static-map** *protocol protocol-address smds-address* [**broadcast**]

<b>Syntax Description</b>	<i>protocol</i>	Higher-level protocol. It can be one of the following values: <b>appletalk</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , <b>ipx</b> , <b>vines</b> , or <b>xns</b> .
	<i>protocol-address</i>	Address of the higher-level protocol.
	<i>smds-address</i>	SMDS address, to complete the mapping.
	<b>broadcast</b>	(Optional) Marks the specified protocol address as a candidate for broadcast packets. All broadcast requests are sent to the unicast SMDS address.





## X.25 and LAPB Commands

---

This chapter describes the function and syntax of the X.25 and LAPB commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Wide-Area Networking Command Reference*.

### access-class (X.25)

To configure an incoming access class on virtual terminals, use the **access-class** (X.25) line configuration command.

```
access-class access-list-number in
```

---

#### Syntax Description

<i>access-list-number</i>	An integer from 1 to 199 that you select for the access list.
<b>in</b>	Restricts incoming connections between a particular access server and the addresses in the access list.

---

### bfe

This command is no longer supported.

### clear x25

To restart an X.25 service or Connection-Mode Network Service (CMNS), to clear a switched virtual circuit (SVC), or to reset a permanent virtual circuit (PVC), use the **clear x25** privileged EXEC command.

```
clear x25 {serial number | {ethernet | fastethernet | tokenring | fdi} number mac-address}  
[vc-number] | [dldci number]
```

Syntax Description		
	<i>serial number</i>	Local serial interface being used for X.25 service.
	<b>ethernet</b>   <b>fastethernet</b>   <b>tokenring</b>   <b>fdi</b> <i>number mac-address</i>	Local CMNS interface (Ethernet, Fast Ethernet, Token Ring, or FDDI interface) and MAC address of the remote device; this information identifies a CMNS service.
	<i>vc-number</i>	(Optional) SVC or PVC number, in the range 1 to 4095. If specified, the SVC is cleared or the PVC is reset. If not specified, the X.25 or CMNS service is restarted.
	<i>dli number</i>	(Optional) When combined with a serial interface number, it triggers a restart event for an Annex G logical X.25 VC.

## clear x25-vc

This command is replaced by the **clear x25** command. See the description of the **clear x25** command earlier in this chapter for more information.

## clear xot

To clear an X.25 over TCP (XOT) switched virtual circuit (SVC) or reset an XOT permanent virtual circuit (PVC), use the **clear xot EXEC** command.

```
clear xot remote ip-address port local ip-address port
```

Syntax Description		
	<b>remote</b> <i>ip-address port</i>	Remote IP address and port number of an XOT connection ID.
	<b>local</b> <i>ip-address port</i>	Local IP address and port number of an XOT connection ID.

## cmns enable

To enable the Connection-Mode Network Service (CMNS) on a nonserial interface, use the **cmns enable** interface configuration command. To disable this capability, use the **no** form of this command.

```
cmns enable
```

```
no cmns enable
```

Syntax Description	
	This command has no arguments or keywords.

## encapsulation lapb

To exchange datagrams over a serial interface using Link Access Procedure, Balanced (LAPB) encapsulation, use the **encapsulation lapb** interface configuration command.

```
encapsulation lapb [dte | dce] [multi | protocol]
```

Syntax Description	
<b>dte</b>	(Optional) Specifies operation as a data terminal equipment (DTE) device. This is the default LAPB mode.
<b>dce</b>	(Optional) Specifies operation as a data communications equipment (DCE) device.
<b>multi</b>	(Optional) Specifies use of multiple local-area network (LAN) protocols to be carried on the LAPB line.
<i>protocol</i>	(Optional) A single protocol to be carried on the LAPB line. A single protocol can be one of the following: <b>apollo</b> , <b>appletalk</b> , <b>clns</b> (ISO CLNS), <b>decnet</b> , <b>ip</b> , <b>ipx</b> (Novell IPX), <b>vines</b> , and <b>xns</b> . IP is the default protocol.

## encapsulation x25

To specify a serial interface's operation as an X.25 device, use the **encapsulation x25** interface configuration command.

```
encapsulation x25 [dte | dce] [ddn | bfe] | [ietf]
```

```
no encapsulation x25 [dte | dce] [ddn | bfe] | [ietf]
```

Syntax Description	
<b>dte</b>	(Optional) Specifies operation as a data terminal equipment (DTE). This is the default X.25 mode.
<b>dce</b>	(Optional) Specifies operation as a data communications equipment (DCE).
<b>ddn</b>	(Optional) Specifies Defense Data Network (DDN) encapsulation on an interface using DDN X.25 Standard Service.
<b>bfe</b>	(Optional) Specifies Blacker Front End (BFE) encapsulation on an interface attached to a BFE device.
<b>ietf</b>	(Optional) Specifies that the interface's datagram encapsulation defaults to use of the Internet Engineering Task Force (IETF) standard method, as defined by RFC 1356.

## lapb interface-outage

To specify the period for which a link will remain connected, even if a brief hardware outage occurs, use the **lapb interface-outage** interface configuration command.

```
lapb interface-outage milliseconds
```

Syntax Description	
<i>milliseconds</i>	Number of milliseconds (ms) a hardware outage can last without the protocol disconnecting the service.

## lapb k

To specify the maximum permissible number of outstanding frames, called the *window size*, use the **lapb k** interface configuration command.

**lapb k** *window-size*

---

### Syntax Description

<i>window-size</i>	Frame count. It can be a value from 1 to the modulo size minus 1 (the maximum is 7 if the modulo size is 8; it is 127 if the modulo size is 128).
--------------------	---

---

## lapb modulo

To specify the Link Access Procedure, Balanced (LAPB) basic (modulo 8) or extended (modulo 128) protocol mode, use the **lapb modulo** interface configuration command.

**lapb modulo** *modulus*

---

### Syntax Description

<i>modulus</i>	Either 8 or 128. The value 8 specifies LAPB's basic mode; the value 128 specifies LAPB's extended mode.
----------------	---

---

## lapb n1

To specify the maximum number of bits a frame can hold (the Link Access Procedure, Balanced [LAPB] N1 parameter), use the **lapb n1** interface configuration command.

**lapb n1** *bits*

---

### Syntax Description

<i>bits</i>	Maximum number of bits in multiples of eight. The minimum and maximum range is dynamically set. Use the question mark (?) to view the range.
-------------	--

---

## lapb n2

To specify the maximum number of times a data frame can be sent (the Link Access Procedure, Balanced [LAPB] N2 parameter), use the **lapb n2** interface configuration command.

**lapb n2** *tries*

---

### Syntax Description

<i>tries</i>	Transmission count. It can be a value from 1 to 255.
--------------	--

---

## lapb protocol

The **lapb protocol** command has been replaced by the [*protocol* | **multi**] option of the **encapsulation lapb** command. See the description of the [*protocol* | **multi**] option of the **encapsulation lapb** command earlier in this chapter for more information.

## lapb t1

To set the retransmission timer period (the Link Access Procedure, Balanced [LAPB] T1 parameter), use the **lapb t1** interface configuration command.

**lapb t1** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Time in milliseconds. It can be a value from 1 to 64000.
---------------------------	---------------------	--

## lapb t4

To set the T4 idle timer, after which the Cisco IOS software sends out a Poll packet to determine whether the link has suffered an unsignaled failure, use the **lapb t4** interface configuration command.

**lapb t4** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds between receipt of the last frame and transmission of the outgoing poll.
---------------------------	----------------	--

## service pad

To enable all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers, use the **service pad** global configuration command. To disable this service, use the **no** form of this command.

**service pad** [*cmns*][*from-xot*][*to-xot*]

**no service pad** [*cmns*][*from-xot*][*to-xot*]

<b>Syntax Description</b>	<i>cmns</i>	(Optional) Specifies sending and receiving PAD calls over CMNS.
	<i>from-xot</i>	(Optional) Accepts XOT to PAD connections.
	<i>to-xot</i>	(Optional) Allows outgoing PAD calls over XOT.

## service pad from-xot

To permit incoming X.25 over TCP (XOT) calls to be accepted as a packet assembler/disassembler (PAD) session, use the **service pad from-xot** global configuration command. To disable this service, use the **no** form of this command.

**service pad from-xot**

**no service pad from-xot**

---

**Syntax Description** This command has no arguments or keywords.

## service pad to-xot

To permit outgoing PAD sessions to use routes to an XOT destination, use the **service pad to-xot** global configuration command. To disable this service, use the **no** form of this command.

**service pad to-xot**

**no service pad to-xot**

---

**Syntax Description** This command has no arguments or keywords.

## show cmns

To display X.25 Level 3 parameters for LAN interfaces (such as Ethernet or Token Ring) and other information pertaining to Connection-Mode Network Service (CMNS) traffic activity, use the **show cmns EXEC** command.

**show cmns** [*type number*]

---

<b>Syntax Description</b>	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

---

## show x25 context

To view operating configuration status details of an X.25 link, use the **show x25 context EXEC** command.

**show x25 context** [*interface number dlcilink number*]

---

<b>Syntax Description</b>	<i>interface number</i>	(Optional) Specific logical X.25 virtual circuit interface.
	<i>dlcilink number</i>	(Optional) Specific DLCI link.

---

## show x25 cug

To display information about all closed user groups (CUGs) or specific CUGs (defined by the local or network CUG number), use the **show x25 cug** EXEC command.

```
show x25 cug {local-cug number | network-cug number}
```

Syntax Description		
	<b>local-cug</b>	Locally significant CUG identifier.
	<i>number</i>	Local CUG number (0 to 9999).
	<b>network-cug</b>	Network translated CUG identifier.
	<i>number</i>	Network CUG number (0 to 9999).

## show x25 hunt-group

To display hunt groups and view detailed interface statistics and distribution methods, use the **show x25 hunt-group** EXEC command.

```
show x25 hunt-group [name]
```

Syntax Description		
	<i>name</i>	(Optional) Displays the specific hunt group named.

## show x25 interface

To display information about virtual circuits (VCs) that use an X.25 interface and, optionally, about a specified virtual circuit, use the **show x25 interface** EXEC command.

```
show x25 interface [serial number | cmns-interface mac mac-address]
```

Syntax Description		
	<i>serial number</i>	(Optional) Keyword <b>serial</b> and number of the serial interface used for X.25.
	<i>cmns-interface mac mac-address</i>	(Optional) Local CMNS interface type and number, plus the MAC address of the remote device. CMNS interface types are Ethernet, Token Ring, or FDDI. The interface numbering scheme depends on the router interface hardware.

## show x25 map

To display information about configured address maps, use the **show x25 map** EXEC command.

```
show x25 map
```

Syntax Description	
	This command has no arguments or keywords.

## show x25 profile

To view details of X.25 profiles on your router, use the **show x25 profile** command in EXEC mode.

```
show x25 profile [name]
```

Syntax Description	
	<i>name</i> (Optional) Name of X.25 profile.

## show x25 remote-red

This command is no longer supported.

## show x25 route

To display the X.25 routing table, use the **show x25 route** EXEC command.

```
show x25 route
```

Syntax Description	
	This command has no arguments or keywords.

## show x25 services

To display information pertaining to the X.25 services, use the **show x25 services** EXEC command.

```
show x25 services
```

Syntax Description	
	This command has no arguments or keywords.

## show x25 vc

To display information about active switched virtual circuits (SVCs) and permanent virtual circuits (PVCs), use the **show x25 vc** EXEC command.

```
show x25 vc [lcn]
```

Syntax Description	
	<i>lcn</i> (Optional) Logical channel number (LCN).

## show x25 xot

To display information for all X.25 over TCP (XOT) virtual circuits that match a given criterion, use the **show x25 xot** EXEC command.

```
show x25 xot [local ip-address [port port]] [remote ip-address [port port]]
```

Syntax	Description
<b>local</b> <i>ip-address</i> [ <b>port</b> <i>port</i> ]	(Optional) Local IP address and optional port number.
<b>remote</b> <i>ip-address</i> [ <b>port</b> <i>port</i> ]	(Optional) Remote IP address and optional port number.

## x25 accept-reverse

To configure the Cisco IOS software to accept all reverse-charge calls, use the **x25 accept-reverse** interface configuration command. To disable this facility, use the **no** form of this command.

```
x25 accept-reverse
```

```
no x25 accept-reverse
```

Syntax	Description
	This command has no arguments or keywords.

## x25 address

To set the X.121 address of a particular network interface, use the **x25 address** interface configuration command.

```
x25 address x121-address
```

Syntax	Description
<i>x121-address</i>	Variable-length X.121 address. It is assigned by the X.25 network service provider.

## x25 alias

To configure an interface alias address that will allow this interface to accept calls with other destination addresses, use the **x25 alias** interface configuration command.

```
x25 alias {destination-pattern | x121-address-pattern} [culd culd-pattern]
```

Syntax Description		
	<i>destination-pattern</i>	Regular expression used to match against the destination address of a received call.
	<i>x121-address-pattern</i>	Alias X.121 address for the interface, allowing it to act as destination host for calls having different destination address.
	<b>cud</b> <i>cud-pattern</i>	(Optional) Call user data (CUD) pattern, a regular expression of ASCII text. The CUD field might be present in a call packet. The first few bytes (commonly 4 bytes long) identify a protocol; the specified pattern is applied to any user data after the protocol identification.

## x25 bfe-decision

This command is no longer supported.

## x25 bfe-emergency

This command is no longer supported.

## x25 default

To set a default protocol that Cisco IOS software will assume applies to incoming calls with unknown or missing protocol identifier in the call user data (CUD), use the **x25 default** interface configuration command. To remove the default protocol specified, use the **no** form of this command.

**x25 default** *protocol*

**no x25 default** *protocol*

Syntax Description		
	<i>protocol</i>	Specifies the protocol to assume; may be <b>ip</b> or <b>pad</b> .

## x25 facility

To force facilities on a per-call basis for calls originated by the router (switched calls are not affected), use the **x25 facility** interface configuration command. To disable a facility, use the **no** form of this command.

**x25 facility option** *value*

**no x25 facility option** *value*

Syntax Description		
	<b>option</b>	Set of user facilities options.
	<i>value</i>	Option value.

## x25 fail-over

To configure a secondary interface and set the number of seconds for which a primary interface must be up before the secondary interface resets, use the **x25 fail-over** command in the appropriate configuration mode. To prevent the secondary interface from resetting, use the **no** form of this command.

**x25 fail-over** *seconds* **interface** *type number* [*dldci* | *mac-address*]

**no x25 fail-over** *seconds* **interface** *type number* [*dldci* | *mac-address*]

Syntax Description		
	<i>seconds</i>	Number of seconds for which the primary interface must be up before the secondary interface resets.
	<b>interface</b>	Secondary interface.
	<i>type</i>	Interface type.
	<i>number</i>	Interface number.
	<i>dldci</i>	(Optional) DLCI number.
	<i>mac-address</i>	(Optional) MAC address.

## x25 hic

To set the highest incoming-only virtual circuit (VC) number, use the **x25 hic** interface configuration command.

**x25 hic** *circuit-number*

Syntax Description		
	<i>circuit-number</i>	VC number from 1 to 4095, or 0 if there is no incoming-only VC range.

## x25 hoc

To set the highest outgoing-only virtual circuit (VC) number, use the **x25 hoc** interface configuration command.

**x25 hoc** *circuit-number*

Syntax Description		
	<i>circuit-number</i>	VC number from 1 to 4095, or 0 if there is no incoming-only VC range.

## x25 hold-queue

To set the maximum number of packets to hold until a virtual circuit (VC) is able to send, use the **x25 hold-queue** interface configuration command. To remove this command from the configuration file and restore the default value, use the **no** form of this command without an argument.

**x25 hold-queue** *packets*

**no x25 hold-queue** [*packets*]

<b>Syntax Description</b>	<i>packets</i>	Number of packets. A hold queue value of 0 allows an unlimited number of packets in the hold queue.
---------------------------	----------------	---

## x25 hold-vc-timer

To start the timer that prevents additional calls to a destination for a given period of time (thus preventing overruns on some X.25 switches caused by Call Request packets), use the **x25 hold-vc-timer** interface configuration command. To restore the default value for the timer, use the **no** form of this command.

**x25 hold-vc-timer** *minutes*

**no x25 hold-vc-timer**

<b>Syntax Description</b>	<i>minutes</i>	Number of minutes that calls to a previously failed destination will be prevented. Incoming calls are still accepted.
---------------------------	----------------	---

## x25 host

To define a static host name-to-address mapping, use the **x25 host** global configuration command. To remove the host name, use the **no** form of the command.

**x25 host** *name x121-address* [ **cud call-user-data**]

**no x25 host** *name*

<b>Syntax Description</b>	<i>name</i>	Host name.
	<i>x121-address</i>	The X.121 address.
	<b> cud call-user-data</b>	(Optional) Sets the Call User Data (CUD) field in the X.25 Call Request packet.

## x25 htc

To set the highest two-way virtual circuit (VC) number, use the **x25 htc** interface configuration command.

```
x25 htc circuit-number
```

<b>Syntax Description</b>	<i>circuit-number</i>	VC number from 1 to 4095, or 0 if there is no two-way VC range.
---------------------------	-----------------------	---

## x25 hunt-group

To create and maintain a hunt group, use the **x25 hunt-group** global configuration command. To delete this hunt group, use the **no** form of this command.

```
x25 hunt-group name {rotary | vc-count}
```

```
no x25 hunt-group name
```

<b>Syntax Description</b>	<i>name</i>	Name you assign to the particular hunt group.
	<b>rotary</b>	Each call steps to the next interface.
	<b>vc-count</b>	Each call is placed on the interface with most available logical channels.

## x25 idle

To define the period of inactivity after which the router can clear a switched virtual circuit (SVC), use the **x25 idle** interface configuration command.

```
x25 idle minutes
```

<b>Syntax Description</b>	<i>minutes</i>	Idle period in minutes.
---------------------------	----------------	-------------------------

## x25 ip-precedence

To enable the Cisco IOS software to use the IP precedence value when it opens a new virtual circuit (VC), use the **x25 ip-precedence** interface configuration command. To cause the Cisco IOS software to ignore the precedence value when opening VCs, use the **no** form of this command.

```
x25 ip-precedence
```

```
no x25 ip-precedence
```

<b>Syntax Description</b>	This command has no arguments or keywords.	
---------------------------	--	--

## x25 ips

To set the interface default maximum input packet size to match that of the network, use the **x25 ips** interface configuration command.

**x25 ips** *bytes*

---

### Syntax Description

<i>bytes</i>	Byte count. It can be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
--------------	--

---

## x25 lic

To set the lowest incoming-only virtual circuit (VC) number, use the **x25 lic** interface configuration command.

**x25 lic** *circuit-number*

---

### Syntax Description

<i>circuit-number</i>	VC number from 1 to 4095, or 0 if there is no incoming-only VC range.
-----------------------	---

---

## x25 linkrestart

To force X.25 Level 3 (packet level) to restart when Level 2 (Link Access Procedure, Balanced [LAPB], the link level) resets, use the **x25 linkrestart** interface configuration command. To disable this function, use the **no** form of this command.

**x25 linkrestart**

**no x25 linkrestart**

---

### Syntax Description

This command has no arguments or keywords.

## x25 loc

To set the lowest outgoing-only virtual circuit (VC) number, use the **x25 loc** interface configuration command.

**x25 loc** *circuit-number*

---

### Syntax Description

<i>circuit-number</i>	VC number from 1 to 4095, or 0 if there is no outgoing-only VC range.
-----------------------	---

---

## x25 ltc

To set the lowest two-way virtual circuit (VC) number, use the **x25 ltc** interface configuration command.

**x25 ltc** *circuit-number*

### Syntax Description

<i>circuit-number</i>	VC number from 1 to 4095, or 0 if there is no two-way VC range.
-----------------------	---

## x25 map

To set up the LAN protocols-to-remote host mapping, use the **x25 map** interface configuration command. To retract a prior mapping, use the **no** form of this command with the appropriate network protocols and X.121 *address* argument.

**x25 map** *protocol address [protocol2 address2 [...[protocol9 address9]]] x121-address [option]*

**no x25 map** *protocol address x121-address*

### Syntax Description

<i>protocol</i>	Protocol type, entered by keyword. Supported protocols are entered by keyword, as listed in Table 3. As many as nine protocol and address pairs can be specified in one command line.
<i>address</i>	Protocol address.
<i>x121-address</i>	X.121 address of the remote host.
<i>option</i>	(Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 4.

Table 3 lists the protocols supported by X.25.

**Table 3** Protocols Supported by X.25

Keyword	Protocol
<b>apollo</b>	Apollo Domain
<b>appletalk</b>	AppleTalk
<b>bridge</b>	Bridging <sup>1</sup>
<b>clns</b>	ISO Connectionless Network Service
<b>compressedtcp</b>	TCP/IP header compression
<b>decnet</b>	DECnet
<b>ip</b>	IP
<b>ipx</b>	Novell IPX
<b>pad</b>	PAD links <sup>2</sup>
<b>qllc</b>	System Network Architecture (SNA) encapsulation in X.25 <sup>3</sup>

**Table 3** *Protocols Supported by X.25 (continued)*

Keyword	Protocol
vines	Banyan VINES
xns	XNS

1. Bridging traffic is supported only for Cisco's traditional encapsulation method, so a bridge map cannot specify other protocols.
2. Packet assembler/disassembler (PAD) maps are used to configure session and protocol translation access, therefore, this protocol is not available for multiprotocol encapsulation.
3. Qualified Logical Link Control (QLLC) is not available for multiprotocol encapsulation.

Table 4 lists the map options supported by X.25 using the **x25 map** command.

**Table 4** *x25 map Options*

Option	Description
<b>accept-reverse</b>	Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls.
<b>broadcast</b>	Causes the Cisco IOS software to direct any broadcasts sent through this interface to the specified X.121 address. This option also simplifies the configuration of OSPF.
<b>cug group-number</b>	Specifies a closed user group (CUG) number (from 1 to 9999) for the mapping in an outgoing call.
<b>compress</b>	Specifies that X.25 payload compression be used for mapping the traffic to this host. Each virtual circuit established for compressed traffic uses a significant amount of memory (for a table of learned data patterns) and for computation (for compression and decompression of all data). Cisco recommends that compression be used with careful consideration of its impact on overall performance.
<b>idle minutes</b>	Specifies an idle timeout for calls other than the interface default; 0 minutes disables the idle timeout.

Table 4 x25 map Options (continued)

Option	Description
<b>method</b> { <b>cisco</b>   <b>ietf</b>   <b>snap</b>   <b>multi</b> }	Specifies the encapsulation method. The choices are as follows: <ul style="list-style-type: none"> <li>• <b>cisco</b>—Cisco’s proprietary encapsulation; not available if more than one protocol is to be carried.</li> <li>• <b>ietf</b>—Default RFC 1356 operation: protocol identification of single-protocol virtual circuits and protocol identification within multiprotocol virtual circuits use the standard encoding, which is compatible with RFC 877. Multiprotocol virtual circuits are used only if needed.</li> <li>• <b>snap</b>—RFC 1356 operation where IP is identified with SNAP rather than the standard IETF method (the standard method is compatible with RFC 877).</li> <li>• <b>multi</b>—Forces a map that specifies a single protocol to set up a multiprotocol virtual circuit when a call is originated; also forces a single-protocol PVC to use multiprotocol data identification methods for all datagrams sent and received.</li> </ul>
<b>no-incoming</b>	Use the map only to originate calls.
<b>no-outgoing</b>	Do not originate calls when using the map.
<b>nudata</b> <i>string</i>	Specifies the network user identification in a format determined by the network administrator (as allowed by the standards). This option is provided for connecting to non-Cisco equipment that requires an NUID facility. The string should not exceed 130 characters and must be enclosed in quotation marks (“ ”) if there are any spaces present. This option only works if the router is configured as an X.25 DTE.
<b>nuid</b> <i>username password</i>	Specifies that a network user ID (NUID) facility be sent in the outgoing call with the specified TACACS username and password (in a format defined by Cisco). This option should be used only when connecting to another Cisco router. The combined length of the username and password should not exceed 127 characters. This option only works if the router is configured as an X.25 data terminal equipment (DTE).
<b>nvc</b> <i>count</i>	Sets the maximum number of virtual circuits for this map or host. The default <i>count</i> is the <b>x25 nvc</b> setting of the interface. A maximum number of eight virtual circuits can be configured for each map. Compressed TCP may use only 1 virtual circuit.
<b>packetsize</b> <i>in-size out-size</i>	Proposes maximum input packet size ( <i>in-size</i> ) and maximum output packet size ( <i>out-size</i> ) for an outgoing call. Both values typically are the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
<b>passive</b>	Specifies that the X.25 interface should send compressed outgoing TCP datagrams only if they were already compressed when they were received. This option is available only for compressed TCP maps.
<b>reverse</b>	Specifies reverse charging for outgoing calls.

Table 4 x25 map Options (continued)

Option	Description
<b>roa name</b>	Specifies the name defined by the <b>x25 roa</b> command for a list of transit Recognized Operating Agencies (ROAs, formerly called Recognized Private Operating Agencies, or RPOAs) to use in outgoing Call Request packets.
<b>throughput in out</b>	Sets the requested throughput class values for input ( <i>in</i> ) and output ( <i>out</i> ) throughput across the network for an outgoing call. Values for <i>in</i> and <i>out</i> are in bits per second (bps) and range from 75 to 48000 bps.
<b>transit-delay milliseconds</b>	Specifies the transit delay value in milliseconds (0 to 65534) for an outgoing call, for networks that support transit delay.
<b>window-size in-size out-size</b>	Proposes the packet count for input window ( <i>in-size</i> ) and output window ( <i>out-size</i> ) for an outgoing call. Both values typically are the same, must be in the range 1 to 127, and must be less than the value set by the <b>x25 modulo</b> command.

## x25 map bridge

To configure an Internet-to-X.121 address mapping for bridging of packets in X.25 frames, use the **x25 map bridge** interface configuration command. Use the **no** form of this command to disable the Internet-to-X.121 address mapping.

```
x25 map bridge x121-address broadcast [option]
```

Syntax	Description
<i>x121-address</i>	The X.121 address.
<b>broadcast</b>	Required keyword for bridging over X.25.
<i>option</i>	(Optional) Services that can be added to this map (same options as the <b>x25 map</b> command).

## x25 map cmns

The **x25 map cmns** command is replaced by the enhanced **x25 route** command. See the description of the **x25 route** command in this chapter for more information.

## x25 map compressedtcp

To map compressed TCP traffic to an X.121 address, use the **x25 map compressedtcp** interface configuration command. To delete a TCP/IP header compression map for the link, use the **no** form of this command.

```
x25 map compressedtcp ip-address [protocol2 address2 [...[protocol9 address9]]]
x121-address [option]
```

```
no x25 map compressedtcp address [protocol2 address2 [...[protocol9 address9]]]
x121-address
```

Syntax Description		
	<i>ip-address</i>	IP address.
	<i>protocol</i>	(Optional) Protocol type, entered by keyword. Supported protocols are entered by keyword, as listed in Table 3 earlier in this chapter. As many as nine protocol and address pairs can be specified in one command line.
	<i>address</i>	(Optional) Protocol address.
	<i>x121-address</i>	X.121 address.
	<i>option</i>	(Optional) The same options as those for the <b>x25 map</b> command; see Table 4 earlier in this chapter.

## x25 map pad

To configure an X.121 address mapping for packet assembler/disassembler (PAD) access over X.25, use the **x25 map pad** interface configuration command.

```
x25 map pad x121-address [option]
```

Syntax Description		
	<i>x121-address</i>	X.121 address of the interface.
	<i>option</i>	(Optional) Services that can be added to this map—the same options as the <b>x25 map</b> command; see Table 4 earlier in this chapter.

## x25 modulo

To set the window modulus, use the **x25 modulo** interface configuration command.

```
x25 modulo modulus
```

Syntax Description		
	<i>modulus</i>	Either 8 or 128. The value of the modulo parameter must agree with that of the device on the other end of the X.25 link.

## x25 nvc

To specify the maximum number of virtual circuits (VCs) that a protocol can have open simultaneously to one host, use the **x25 nvc** interface configuration command. To increase throughput across networks, you can establish up to eight virtual circuits to a host and protocol.

**x25 nvc** *count*

---

### Syntax Description

<i>count</i>	Circuit count from 1 to 8. A maximum of eight virtual circuits can be configured for each protocol-host pair. Protocols that do not tolerate out-of-sequence delivery, such as encapsulated TCP/IP header compression, will use only one virtual circuit despite this value. Permitting more than one VC may help throughput on slow networks.
--------------	--

---

## x25 ops

To set the interface default maximum output packet size to match that of the network, use the **x25 ops** interface configuration command.

**x25 ops** *bytes*

---

### Syntax Description

<i>bytes</i>	Byte count that is one of the following: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
--------------	--

---

## x25 pad-access

To cause the packet assembler/disassembler (PAD) software to accept PAD connections only from statically mapped X.25 hosts, use the **x25 pad-access** interface configuration command. To disable checking maps on PAD connections, use the **no** form of this command.

**x25 pad-access**

**no x25 pad-access**

---

### Syntax Description

This command has no arguments or keywords.

## x25 profile

To configure an X.25 profile without allocating any hardware specific information, use the **x25 profile** command in global configuration mode. To delete this profile, use the **no** form of this command.

**x25 profile** *name* {**dce** | **dte** | **dxe**}

**no x25 profile** *name*

Syntax Description		
	<i>name</i>	X.25 profile name that you assign.
	<b>dce</b>	Indicates a data communications equipment (DCE) interface.
	<b>dte</b>	Indicates a data terminal equipment (DTE) interface.
	<b>dxe</b>	Indicates a data exchange equipment (DXE) interface.

## x25 pvc (encapsulation)

To establish an encapsulation permanent virtual circuit (PVC), use the encapsulating version of the **x25 pvc** interface configuration command. To delete the PVC, use the **no** form of this command with the appropriate channel number.

```
x25 pvc circuit protocol address [protocol2 address2 [...[protocol9 address9]]] x121-address
[option]
```

```
no x25 pvc circuit
```

Syntax Description		
	<i>circuit</i>	Virtual-circuit channel number, which must be less than the virtual circuits assigned to the switched virtual circuits (SVCs).
	<i>protocol</i>	Protocol type, entered by keyword. Supported protocols are listed in Table 5. As many as nine protocol and address pairs can be specified in one command line.
	<i>address</i>	Protocol address of the host at the other end of the PVC.
	<i>x121-address</i>	X.121 address.
	<i>option</i>	(Optional) Provides additional functionality or allows X.25 parameters to be specified for the PVC. Can be any of the options listed in Table 6.

**Table 5** Protocols Supported by X.25 PVCs

Keyword	Protocol
<b>apollo</b>	Apollo Domain
<b>appletalk</b>	AppleTalk
<b>bridge</b>	Bridging <sup>1</sup>
<b>clns</b>	OSI Connectionless Network Service
<b>compressedtcp</b>	TCP/IP header compression
<b>decnet</b>	DECnet
<b>ip</b>	IP
<b>ipx</b>	Novell IPX
<b>qllc</b>	SNA encapsulation in X.25 <sup>2</sup>
<b>vines</b>	Banyan VINES
<b>xns</b>	XNS

1. Bridging traffic is supported only for Cisco's traditional encapsulation method, so a bridge PVC cannot specify other protocols.
2. QLLC is not available for multiprotocol encapsulation.

Table 6 lists supported X.25 PVC options.

**Table 6** x25 pvc Options

Option	Description
<b>broadcast</b>	Causes the Cisco IOS software to direct any broadcasts sent through this interface to this PVC. This option also simplifies the configuration of OSPF.
<b>method</b> { <b>cisco</b>   <b>ietf</b>   <b>snap</b>   <b>multi</b> }	Specifies the encapsulation method. The choices are as follows: <ul style="list-style-type: none"> <li>• <b>cisco</b>—Single protocol encapsulation; not available if more than one protocol is carried.</li> <li>• <b>ietf</b>—Default RFC 1356 operation; single-protocol encapsulation unless more than one protocol is carried, and protocol identification when more than one protocol is carried.</li> <li>• <b>snap</b>—RFC 1356 operation where IP is identified when more than one protocol is carried using the SNAP encoding.</li> <li>• <b>multi</b>—Multiprotocol encapsulation used on the PVC.</li> </ul>
<b>packetsize</b> <i>in-size</i> <i>out-size</i>	Maximum input packet size ( <i>in-size</i> ) and output packet size ( <i>out-size</i> ) for the PVC. Both values are typically the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
<b>passive</b>	Specifies that transmitted TCP datagrams will be compressed only if they were received compressed. This option is available only for PVCs carrying compressed TCP/IP header traffic.
<b>windowsize</b> <i>in-size</i> <i>out-size</i>	Packet count for input window ( <i>in-size</i> ) and output window ( <i>out-size</i> ) for the PVC. Both values are typically the same, must be in the range 1 to 127, and must be less than the value set for the <b>x25 modulo</b> command.

## x25 pvc (switched)

To configure a switched permanent virtual circuit (PVC) for a given interface, use the switched version of the **x25 pvc** interface configuration command.

```
x25 pvc number1 interface type number pvc number2 [option]
```

Syntax Description	
<i>number1</i>	PVC number that will be used on the local interface (as defined by the primary interface command).
<b>interface</b>	Required keyword to specify an interface.
<i>type</i>	Remote interface type.
<i>number</i>	Remote interface number.
<b>pvc</b>	Required keyword to specify a switched PVC.
<i>number2</i>	PVC number that will be used on the remote interface.
<i>option</i>	(Optional) Adds certain features to the mapping specified; can be either option listed in Table 7.

Table 7 lists the switched PVC options supported by X.25.

**Table 7** x25 pvc Switched PVC Options

Option	Description
<b>packetsize</b> <i>in-size out-size</i>	Maximum input packet size ( <i>in-size</i> ) and output packet size ( <i>out-size</i> ) for the PVC. Both values must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
<b>windowsize</b> <i>in-size out-size</i>	Packet count for input window ( <i>in-size</i> ) and output window ( <i>out-size</i> ) for the PVC. Both values should be the same, must be in the range 1 to 127, and must not be greater than the value set for the <b>x25 modulo</b> command.

## x25 pvc (switched PVC to SVC)

To configure a switched permanent virtual circuit (PVC) to a switched virtual circuit (SVC) for a given interface, use the switched PVC to SVC version of the **x25 pvc** interface configuration command.

```
x25 pvc number1 svc x121-address [flow-control-options] [call-control-options]
```

### Syntax Description

<i>number1</i>	Logical channel ID of the PVC. Value must be lower than any range of circuit numbers defined for SVCs.
<b>svc</b>	Specifies a SVC type.
<i>x121-address</i>	Destination X.121 address for opening an outbound SVC and source X.121 address for matching an inbound SVC.
<i>flow-control-options</i>	(Optional) Adds certain features to the mapping specified. It can be any of the options listed in Table 8.
<i>call-control-options</i>	(Optional) Adds certain features to the mapping specified. It can be any of the options listed in Table 9.

Table 8 lists the flow control options supported by X.25 during PVC to SVC switching.

**Table 8** x25 pvc Flow Control Options

Option	Description
<b>packetsize</b> <i>in-size out-size</i>	Maximum input packet size ( <i>in-size</i> ) and output packet size ( <i>out-size</i> ) for both the PVC and SVC. Values may differ but must be one of the following: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
<b>windowsize</b> <i>in-size out-size</i>	Packet count for input window ( <i>in-size</i> ) and output window ( <i>out-size</i> ) for both the PVC and SVC. Both values may differ but must be in the range 1 to 127 and must be less than the value set for the <b>x25 modulo</b> command.

Table 9 lists the call control options supported by X.25 during PVC to SVC switching.

Table 9 x25 pvc Call Control Options

Option	Description
<b>accept-reverse</b>	Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls.
<b>idle minutes</b>	Idle time-out for the SVC. This option will override the interface's <b>x25 idle</b> command value only for this circuit.
<b>no-incoming</b>	Establishes a switched virtual circuit to the specified X.121 address when data is received from the permanent virtual circuit, but does not accept calls from this X.121 address.
<b>no-outgoing</b>	Accepts an incoming call from the specified X.121 address, but does not attempt to place a call when data is received from the permanent virtual circuit. If data is received from the permanent virtual circuit while no call is connected, the PVC will be reset.

## x25 pvc (XOT)

To connect two permanent virtual circuits (PVCs) across a TCP/IP LAN, use the X.25-over-TCP (XOT) service form of the **x25 pvc** interface configuration command.

**x25 pvc** *number1* **xot** *address* **interface serial** *string* **pvc** *number2* [*option*]

### Syntax Description

<i>number1</i>	PVC number of the connecting device.
<b>xot</b>	Indicates two PVCs will be connected across a TCP/IP LAN using XOT.
<i>address</i>	IP address of the device to which you are connecting.
<b>interface serial</b>	Indicates the interface is serial.
<i>string</i>	Serial interface specification that accepts either a number or a string in model 7000 format ( <i>number/number</i> ) to denote the serial interface.
<b>pvc</b>	Indicates a PVC.
<i>number2</i>	Remote PVC number on the target interface.
<i>option</i>	(Optional) Adds certain features for the connection; can be one or more of the options listed in Table 10.

Table 10 lists the PVC tunnel options supported by X.25.

Table 10 x25 pvc PVC Tunnel Options

Option	Description
<b>packetsize</b> <i>in-size out-size</i>	Maximum input packet size ( <i>in-size</i> ) and output packet size ( <i>out-size</i> ) for the PVC. Both values must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
<b>window</b> <i>in-size out-size</i>	Packet count for input window ( <i>in-size</i> ) and output window ( <i>out-size</i> ) for the PVC. Both values should be the same, must be in the range 1 to 127, and must not be greater than or equal to the value set for the <b>x25 modulo</b> command.
<b>xot-keepalive-period</b> <i>seconds</i>	Number of seconds between keepalives for XOT connections. The default is 60 seconds.
<b>xot-keepalive-tries</b> <i>count</i>	Number of times TCP keepalives should be sent before dropping the connection. The default value is 4 times.
<b>xot-promiscuous</b>	Indicates that the remote IP address should be ignored when matching an incoming XOT connection with the XOT PVC parameters.
<b>xot-source</b> <i>interface</i>	Specifies an interface whose IP address should be used as the local IP address of the TCP connection.

## x25 remote-red

This command is no longer supported.

## x25 retry

To activate a secondary route while also retrying a failed primary route, use the **x25 retry** interface configuration command in conjunction with the `ip route` or `backup interface` commands. To discontinue implementing secondary X.25 routes and retrying of primary X.25 routes, use the **no** form of this command.

**x25 retry interval** *seconds attempts count*

**no x25 retry interval** *seconds attempts count*

### Syntax Description

<b>interval</b>	Keyword defining interval between attempts.
<i>seconds</i>	Number of seconds between attempts.
<b>attempts</b>	Keyword defining number of attempts.
<i>count</i>	Number of attempts to reestablish the closed link before discontinuing.

## x25 roa

To specify a sequence of packet network carriers, use the **x25 roa** global configuration command. To remove the specified name, use the **no** form of this command.

**x25 roa** *name number*

**no x25 roa** *name*

Syntax Description		
	<i>name</i>	Recognized Operating Agency (ROA, formerly called a Recognized Private Operating Agency, or RPOA), which must be unique with respect to all other ROA names. It is used in the <b>x25 facility</b> and <b>x25 map</b> interface configuration commands.
	<i>number</i>	A sequence of 1 or more numbers used to describe an ROA; up to 10 numbers are accepted.

## x25 route

To create an entry in the X.25 routing table (to be consulted for forwarding incoming calls and for placing outgoing packet assembler/disassembler (PAD) or protocol translation calls), use the appropriate form of the **x25 route** global configuration command. To remove an entry from the table, use the **no** form of the command.

**x25 route** [*#position*] [*selection-options*] [*modification-options*] *disposition-options*  
[*xot-keepalive-options*]

**no x25 route** [*#position*] [*selection-options*] [*modification-options*] *disposition-options*  
[*xot-keepalive-options*]

Syntax Description		
	<i>#position</i>	(Optional) A pound sign (#) followed by a number designates the position in the routing table at which to insert the new entry. If no value for the <i>position</i> argument is given, the entry is appended to the end of the routing table.
	<i>selection-options</i>	(Optional) The selection options identify when the subsequent modification and disposition options apply to an X.25 call; any or all variables may be specified for a route. For selection keyword and argument options, see Table 11.  For selection and modification pattern and character matching and replacement see Table 13, Table 14, and Table 15.  Although each individual selection criterion is optional, at least one selection or modification option must be specified in the <b>x25 route</b> command.

<i>modification-options</i>	<p>(Optional) The modification options modify the source or destination addresses of the selected calls. The standard regular expression substitution rules are used, where a match pattern and rewrite string direct the construction of a new string. For modification keyword and argument options, see Table 12.</p> <p>For selection and modification pattern and character matching and replacement see Table 13, Table 14, and Table 15.</p> <p>Although each individual modification is optional, at least one selection or modification option must be specified in the <b>x25 route</b> command.</p>
<i>disposition-options</i>	Specifies the disposition of a call matching the specified selection pattern. For disposition keyword and argument options, see Table 16.
<i>xot-keepalive-options</i>	<p>(Optional) The XOT-keepalive options specify an X.25 over TCP (XOT) keepalive period and number of XOT-keepalive retries. XOT relies on TCP to detect when the underlying connection is dead. TCP detects a dead connection when sent data goes unacknowledged for a given number of attempts over a period of time. For XOT-keepalive keyword and argument options, see Table 17.</p>

Table 11 lists the selection options for the **x25 route** command. At least one selection or modification option must be specified.

**Table 11** x25 route Selection Options

Selection Option	Description
<b>cmd</b> <i>user-data-pattern</i>	(Optional) CUD pattern, which is specified as a regular expression of printable ASCII text. The CUD field may be present in a call packet. The first few bytes (commonly 4 bytes long) identify a protocol; the specified pattern is applied to any user data after the protocol identification.
<i>destination-pattern</i>	(Optional) Destination address pattern, which is a regular expression that can represent either one X.121 address (such as ^1111000\$) or any address in a group of X.121 addresses (such as ^1111.*).
<b>dest-ext</b> <i>nsap-destination-pattern</i>	<p>(Optional) NSAP destination address pattern, which is a regular expression that can represent either an NSAP destination address (such as ^11.1111.0000\$) or an NSAP prefix (such as ^11.1111.*).</p> <p> <b>Note</b> A period (.) in the pattern is interpreted as a character wildcard, which will not interfere with a match to the actual period in the NSAP; if desired, an explicit character match may be used (such as ^11\1111\.*).</p>
<b>hunt-group</b> <i>name</i>	Routes the selected call to the X.25 hunt group. The chosen router may vary depending on the hunt group configuration.

**Table 11** x25 route Selection Options (continued)

Selection Option	Description
<b>input interface</b> <i>interface number</i>	(Optional) Specifies interface number on which the call will be received.
<b>source</b> <i>source-pattern</i>	(Optional) Source address pattern, which is a regular expression that can represent either one X.121 source address (such as ^2222000\$) or any address in a group of X.121 addresses (such as ^2222.*).

Table 12 lists the modification options for the **x25 route** command. At least one selection or modification option must be specified.

**Table 12** x25 route Modification Options

Modification Option	Description
<b>substitute-dest</b> <i>rewrite-dest</i>	(Optional) Called X.121 address rewrite pattern.  The destination address, <i>destination-pattern</i> , and this <i>rewrite-dest</i> pattern are used to form a new destination address. If no <i>destination-pattern</i> is specified, a default match pattern of .* is used.  See Table 13 and Table 14 for summaries of pattern and character matching, respectively. See Table 15 for a summary of pattern rewrite elements.
<b>substitute-source</b> <i>rewrite-source</i>	(Optional) Calling X.121 address rewrite pattern.  The <i>source address</i> , <i>source-pattern</i> , and this <i>rewrite-source</i> pattern are used to form a new source address. If no <i>source-pattern</i> is specified, any <i>destination-pattern</i> match pattern is used. If neither match pattern is specified, a default match pattern of .* is used.  See Table 13 and Table 14 for summaries of pattern and character matching, respectively. See Table 15 for a summary of pattern rewrite elements.

See Table 13, Table 14, and Table 15, respectively, for summaries of pattern matching, character matching, and pattern replacement elements. Note that up to nine pairs of parentheses can be used to identify patterns to be included in the modified string. A more complete description of the pattern-matching characters is found in the “Regular Expressions” appendix in the *Cisco IOS Terminal Services Configuration Guide*.

**Table 13** Pattern Matching for x25 route Selection and Modification Options

Pattern	Description
*	Matches 0 or more occurrences of the preceding character.
+	Matches 1 or more occurrences of the preceding character.
?	Matches 0 or 1 occurrences of the preceding character. <sup>1</sup>

1. Precede the question mark with **Ctrl-V** to prevent the question mark from being interpreted as a **help** command.

**Table 14 Character Matching for x25 route Selection and Modification Options**

Character	Description
^	Matches the beginning of the input string.
\$	Matches the end of the input string.
\char	Matches the single character <i>char</i> specified.
.	Matches any single character.

**Table 15 Pattern Replacements for x25 route Selection and Modification Options**

Pattern	Description
\0	The pattern is replaced by the entire original address.
\1...9	The pattern is replaced by strings that match the first through ninth parenthetical part of the X.121 address.

Table 16 lists the disposition options for the **x25 route** command. You must select one of these options.

**Table 16 x25 route Disposition Options**

Disposition Option	Description
<b>clear</b>	Terminates the call.
<b>continue</b>	(Optional) Combines sequential route table lookups, holding onto any “selections” and “modifications” specified on the <b>x25 route</b> statement.
<b>hunt-group</b> <i>name</i>	Routes the selected call to the X.25 hunt group. The chosen route may vary depending on the hunt group configuration.
<b>interface</b> <i>interface number</i>	Routes the selected call to the specified X.25 serial interface.
<b>interface</b> <i>interface number dlc</i> <i>number</i>	(Optional) Routes the X.25 call to the specified Annex G link. You must include the interface number and enter the data link connection identifier (DLCI) number. You only need to do this if you want the router to accept switched calls, as well as originate them.
<b>interface</b> <i>cmns-interface</i> <b>mac</b> <i>mac-address</i>	Routes the selected call out the specified broadcast interface via CMNS to the LAN destination station. The broadcast interface type can be Ethernet, Token Ring, or FDDI. The interface numbering scheme depends on the router interface hardware.
<b>xot</b> <i>ip-address</i> [ <i>ip2-address</i> [... <i>ip6-address</i> ]] [ <b>xot-source</b> <i>interface</i> ]	Routes the selected call to the XOT host at the specified IP address. Subsequent IP addresses are tried, in sequence, only if XOT is unable to establish a TCP connection with a prior address.
<b>xot</b> <i>dns pattern</i>	Used with DNS-based X.25 routing, this option consults the DNS to get up to six destination IP addresses using whatever lookup pattern you choose (see Table 15).

Table 17 lists and describes the xot-keepalive options for the **x25 route** command.

**Table 17** x25 route XOT-Keepalive Options

XOT-Keepalive Option	Description
<b>xot-keepalive-period</b> <i>seconds</i>	Number of seconds between keepalives for XOT connections. The default is 60 seconds.
<b>xot-keepalive-tries</b> <i>count</i>	Number of times TCP keepalives should be sent before dropping the connection. The default value is 4 times.

## x25 routing

To enable X.25 switching or tunneling, use the **x25 routing** global configuration command. To disable the forwarding of X.25 calls, use the **no** form of this command.

```
x25 routing [acknowledge local | acknowledge end-to-end] [tcp-use-if-defs]
```

```
no x25 routing [acknowledge local | acknowledge end-to-end] [tcp-use-if-defs]
```

### Syntax Description

<b>acknowledge local</b>	(Optional) Sets local acknowledgment on the router.
<b>acknowledge end-to-end</b>	(Optional) Sets end-to-end acknowledgment. (Default acknowledge setting.)
<b>tcp-use-if-defs</b>	(Optional) Accepts calls received over TCP.

## x25 subscribe cug-service

To enable and control standard closed user group (CUG) behavior on an X.25 data communications equipment (DCE) interface or X.25 profile, use the **x25 subscribe cug-service** interface configuration command. To disable standard CUG behavior on an X.25 DCE interface, use the **no** form of this command.

```
x25 subscribe cug-service [incoming-access | outgoing-access] [suppress preferential |
suppress all]
```

```
no x25 subscribe cug-service [incoming-access | outgoing-access] [suppress preferential |
suppress all]
```

### Syntax Description

<b>incoming-access</b>	(Optional) Allows incoming access from the open network to the data terminal equipment (DTE) device.
<b>outgoing-access</b>	(Optional) Allows outgoing access from the DTE device to the open network.
<b>suppress preferential</b>	(Optional) Suppresses CUG selection facility for the preferential CUG.
<b>suppress all</b>	(Optional) Suppresses CUG selection facility for all CUGs.

## x25 subscribe flow-control

To control flow control parameter negotiation facilities in call setup packets, use the **x25 subscribe flow-control** interface configuration command. To have flow control parameter negotiation facilities included in call setup (outgoing) packets only when their values differ from the default values, use the **no** form of this command.

```
x25 subscribe flow-control {always | never}
```

```
no x25 subscribe flow-control
```

### Syntax Description

<b>always</b>	Flow control parameter negotiation facilities are enabled and the flow control parameters are always included with call setup packets and are optional on inbound packets.
<b>never</b>	Flow control parameter negotiation facilities are disabled and the flow control parameters are never included with call setup packets, and are not permitted on inbound packets. Negotiation of flow control parameters is disabled.

## x25 subscribe local-cug

To configure a data circuit-terminating equipment (DCE) X.25 interface for a specific closed user group (CUG) subscription, use the **x25 subscribe local-cug** interface configuration command. To disable the interface for a specific CUG subscription, use the **no** form of this command.

```
x25 subscribe local-cug number network-cug number [no-incoming | no-outgoing | preferential]
```

```
no x25 subscribe local-cug number network-cug number [no-incoming | no-outgoing | preferential]
```

### Syntax Description

<i>number</i>	Specific local CUG number (0 to 9999).
<b>network-cug</b>	Network translated CUG identifier.
<i>number</i>	Specific network CUG number (0 to 9999).
<b>no-incoming</b>	(Optional) Calls to data terminal equipment (DTE) barred within the specified CUG, unless <b>x25 subscribe cug-service incoming-access</b> is configured.
<b>no-outgoing</b>	(Optional) Calls from DTE barred within the specified CUG, unless <b>x25 subscribe cug-service outgoing-access</b> is configured.
<b>preferential</b>	(Optional) Specified on only one CUG, and is the assumed CUG when none is provided in call setup. (A single CUG listed at the interface is automatically considered a preferential CUG.)

## x25 subscribe packetsize

To set permitted and target ranges for packet size during flow control negotiation, use the **x25 subscribe packetsize** interface configuration command. To revert to the default packet size ranges, use the **no** form of this command.

```
x25 subscribe packetsize { permit pmin pmax | target pmin pmax }
```

```
no x25 subscribe packetsize { permit pmin pmax | target pmin pmax }
```

### Syntax Description

<b>permit</b>	Permitted packet-size range identifier.
<i>pmin</i>	Minimum setting for packet size range (16 to 4096 by a power of two).
<i>pmax</i>	Maximum setting for packet size range (16 to 4096 by a power of two).
<b>target</b>	Target packet-size range identifier.

## x25 subscribe window size

To set permitted and target ranges for window size during flow control negotiation, use the **x25 subscribe window size** interface configuration command. To revert to the default window size ranges, use the **no** form of this command.

```
x25 subscribe window size { permit wmin wmax | target wmin wmax }
```

```
no x25 subscribe window size { permit wmin wmax | target wmin wmax }
```

### Syntax Description

<b>permit</b>	Permitted window size range identifier.
<i>wmin</i>	Minimum setting for window size range (1 to 127).
<i>wmax</i>	Maximum setting for window size range (1 to 127).
<b>target</b>	Target window-size range identifier.

## x25 suppress-called-address

To omit the destination address in outgoing calls, use the **x25 suppress-called-address** interface configuration command. To reset this command to the default state, use the **no** form of this command.

```
x25 suppress-called-address
```

```
no x25 suppress-called-address
```

### Syntax Description

This command has no arguments or keywords.

## x25 suppress-calling-address

To omit the source address in outgoing calls, use the **x25 suppress-calling-address** interface configuration command. To reset this command to the default state, use the **no** form of this command.

**x25 suppress-calling-address**

**no x25 suppress-calling-address**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## x25 t10

To set the value of the Restart Indication retransmission timer (T10) on data communications equipment (DCE) devices, use the **x25 t10** interface configuration command.

**x25 t10** *seconds*

---

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds.
---------------------------	----------------	-------------------

---

## x25 t11

To set the value of the Incoming Call timer (T11) on data communications equipment (DCE) devices, use the **x25 t11** interface configuration command.

**x25 t11** *seconds*

---

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds.
---------------------------	----------------	-------------------

---

## x25 t12

To set the value of the Reset Indication retransmission timer (T12) on data communications equipment (DCE) devices, use the **x25 t12** interface configuration command.

**x25 t12** *seconds*

---

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds.
---------------------------	----------------	-------------------

---

## x25 t13

To set the value of the Clear Indication retransmission timer (T13) on data communications equipment (DCE) devices, use the **x25 t13** interface configuration command.

**x25 t13** *seconds*

Syntax Description	<i>seconds</i>	Time, in seconds.
--------------------	----------------	-------------------

## x25 t20

To set the value of the Restart Request retransmission timer (T20) on data terminal equipment (DTE) devices, use the **x25 t20** interface configuration command.

**x25 t20** *seconds*

Syntax Description	<i>seconds</i>	Time in seconds.
--------------------	----------------	------------------

## x25 t21

To set the value of the Call Request timer (T21) on data terminal equipment (DTE) devices, use the **x25 t21** interface configuration command.

**x25 t21** *seconds*

Syntax Description	<i>seconds</i>	Time, in seconds.
--------------------	----------------	-------------------

## x25 t22

To set the value of the Reset Request retransmission timer (T22) on data terminal equipment (DTE) devices, use the **x25 t22** interface configuration command.

**x25 t22** *seconds*

Syntax Description	<i>seconds</i>	Time, in seconds.
--------------------	----------------	-------------------

## x25 t23

To set the value of the Clear Request retransmission timer (T23) on data terminal equipment (DTE) devices, use the **x25 t23** interface configuration command.

**x25 t23** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds.
---------------------------	----------------	-------------------

## x25 threshold

To set the data packet acknowledgment threshold, use the **x25 threshold** interface configuration command.

**x25 threshold** *delay-count*

<b>Syntax Description</b>	<i>delay-count</i>	Value between zero and the input window size. A value of 1 sends one Receiver Ready acknowledgment per packet.
---------------------------	--------------------	--

## x25 use-source-address

To override the X.121 addresses of outgoing calls forwarded over a specific interface, use the **x25 use-source-address** interface configuration command. To prevent updating the source addresses of outgoing calls, use the **no** form of this command.

**x25 use-source-address**

**no x25 use-source-address**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## x25 win

To change the default incoming window size to match that of the network, use the **x25 win** interface configuration command.

**x25 win** *packets*

<b>Syntax Description</b>	<i>packets</i>	Packet count that can range from 1 to one less than the window modulus.
---------------------------	----------------	---

## x25 wout

To change the default outgoing window size to match that of the network, use the **x25 wout** interface configuration command.

**x25 wout** *packets*

Syntax Description		
	<i>packets</i>	Packet count that can range from 1 to one less than the window modulus.

## x29 access-list

To limit access to the access server from certain X.25 hosts, use the **x29 access-list** global configuration command. To delete an entire access list, use the **no** form of this command.

**x29 access-list** *access-list-number* { **deny** | **permit** } *x121-address*

**no x29 access-list** *access-list-number*

Syntax Description		
	<i>access-list-number</i>	Number of the access list. It can be a value between 1 and 199.
	<b>deny</b>	Denies access and clears call requests immediately.
	<b>permit</b>	Permits access to the protocol translator.
	<i>x121-address</i>	If applied as an inbound access class, specifies the X.121 address that can or cannot have access (with or without regular expression pattern-matching characters). The X.121 address is the source address of the incoming packet.  If applied as an outbound access class, then the address specifies a destination to where connections are allowed.

## x29 profile

To create a packet assembler/disassembler (PAD) profile script for use by the **translate** command, use the **x29 profile** global configuration command.

**x29 profile** { **default** | *name* } *parameter:value* [*parameter:value*]

Syntax Description		
	<b>default</b>	Specifies default profile script.
	<i>name</i>	Name of the PAD profile script.
	<i>parameter:value</i>	X.3 PAD parameter number and value separated by a colon. You can specify multiple parameter-value pairs on the same line.



## **Security**





# Authentication Commands

This chapter describes the function and syntax of the authentication commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

## aaa authentication arap

To enable an authentication, authorization, and accounting (AAA) authentication method for AppleTalk Remote Access (ARA), use the **aaa authentication arap** command in global configuration mode. To disable this authentication, use the **no** form of this command.

```
aaa authentication arap {default | list-name} method1 [method2...]
```

```
no aaa authentication arap {default | list-name} method1 [method2...]
```

### Syntax Description

<b>default</b>	Uses the listed methods that follow this argument as the default list of methods when a user logs in.
<i>list-name</i>	Character string used to name the following list of authentication methods tried when a user logs in.
<i>method1</i> [ <i>method2...</i> ]	At least one of the keywords described in Table 18.

**Table 18** *aaa authentication arap* Methods

Keyword	Description
<b>guest</b>	Allows guest logins. This method must be the first method listed, but it can be followed by other methods if it does not succeed.
<b>auth-guest</b>	Allows guest logins only if the user has already logged in to EXEC. This method must be the first method listed, but can be followed by other methods if it does not succeed.
<b>line</b>	Uses the line password for authentication.
<b>local</b>	Uses the local username database for authentication.
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.

**Table 18** *aaa authentication arap Methods (continued)*

Keyword	Description
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> command.

## aaa authentication banner

To configure a personalized banner that will be displayed at user login, use the **aaa authentication banner** command in global configuration mode. To remove the banner, use the **no** form of this command.

**aaa authentication banner** *dstringd*

**no aaa authentication banner**

Syntax Description		
<i>d</i>	Any delimiting character at the beginning and end of the <i>string</i> that notifies the system that the <i>string</i> is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.	
<i>string</i>	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.	

## aaa authentication enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine if a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

**aaa authentication enable default** *method1* [*method2...*]

**no aaa authentication enable default** *method1* [*method2...*]

Syntax Description	
<i>method1</i> [ <i>method2...</i> ]	At least one of the keywords described in Table 19.

**Table 19** *aaa authentication enable default Methods*

Keyword	Description
<b>enable</b>	Uses the enable password for authentication.
<b>line</b>	Uses the line password for authentication.
<b>none</b>	Uses no authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.

Table 19 aaa authentication enable default Methods (continued)

Keyword	Description
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> command.

## aaa authentication fail-message

To configure a personalized banner that will be displayed when a user fails login, use the **aaa authentication fail-message** command in global configuration mode. To remove the failed login message, use the **no** form of this command.

```
aaa authentication fail-message dstringd
```

```
no aaa authentication fail-message
```

Syntax Description		
<i>d</i>	The delimiting character at the beginning and end of the <i>string</i> that notifies the system that the <i>string</i> is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.	
<i>string</i>	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.	

## aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

```
aaa authentication login {default | list-name} method1 [method2...]
```

```
no aaa authentication login {default | list-name} method1 [method2...]
```

Syntax Description		
<b>default</b>	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.	
<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.	
<i>method1</i> [ <i>method2</i> ...]	At least one of the keywords described in Table 20.	

**Table 20** *aaa authentication login Methods*

Keyword	Description
<b>enable</b>	Uses the enable password for authentication.
<b>krb5</b>	Uses Kerberos 5 for authentication.
<b>krb5-telnet</b>	Uses Kerberos 5 telnet authentication protocol when using Telnet to connect to the router.
<b>line</b>	Uses the line password for authentication.
<b>local</b>	Uses the local username database for authentication.
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>none</b>	Uses no authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> command.

## aaa authentication nasi

To specify authentication, authorization, and accounting (AAA) authentication for Netware Asynchronous Services Interface (NASI) clients connecting through the access server, use the **aaa authentication nasi** command in global configuration mode. To disable authentication for NASI clients, use the **no** form of this command.

```
aaa authentication nasi {default | list-name} method1 [method2...]
```

```
no aaa authentication nasi {default | list-name} method1 [method2...]
```

### Syntax Description

<b>default</b>	Makes the listed authentication methods that follow this argument the default list of methods used when a user logs in.
<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.
<i>method1</i> [ <i>method2...</i> ]	At least one of the methods described in Table 21.

**Table 21** *aaa authentication nasi Methods*

Keyword	Description
<b>enable</b>	Uses the enable password for authentication.
<b>line</b>	Uses the line password for authentication.
<b>local</b>	Uses the local username database for authentication.
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>none</b>	Uses no authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.

Table 21 *aaa authentication nasi Methods (continued)*

Keyword	Description
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication.
<b>group group-name</b>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> command.

## aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

```
aaa authentication password-prompt text-string
```

```
no aaa authentication password-prompt text-string
```

Syntax Description	<i>text-string</i>	String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, "Enter your password:").
--------------------	--------------------	---

## aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

```
aaa authentication ppp {default | list-name} method1 [method2...]
```

```
no aaa authentication ppp {default | list-name} method1 [method2...]
```

Syntax Description	<b>default</b>	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
	<i>list-name</i>	Character string used to name the list of authentication methods tried when a user logs in.
	<i>method1</i> [ <i>method2</i> ...]	At least one of the keywords described in Table 22.

Table 22 *aaa authentication ppp Methods*

Keyword	Description
<b>if-needed</b>	Does not authenticate if user has already been authenticated on a tty line.
<b>krb5</b>	Uses Kerberos 5 for authentication (can only be used for PAP authentication).
<b>local</b>	Uses the local username database for authentication.

Table 22 *aaa authentication ppp Methods (continued)*

Keyword	Description
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>none</b>	Uses no authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> command.

## aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

**aaa authentication username-prompt** *text-string*

**no aaa authentication username-prompt** *text-string*

### Syntax Description

<i>text-string</i>	String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, "Enter your name:").
--------------------	---

## aaa dnis map authentication ppp group

To map a Dialed Number Information Service (DNIS) number to a particular authentication server group (this server group will be used for authentication, authorization, and accounting (AAA) authentication), use the **aaa dnis map authentication ppp group** command in global configuration mode. To remove the DNIS number from the defined server group, use the **no** form of this command.

**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*

**no aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*

### Syntax Description

<i>dnis-number</i>	Number of the DNIS.
<i>server-group-name</i>	Character string used to name a group of security servers associated in a server group.

## aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

```
aaa new-model
```

```
no aaa new-model
```

**Syntax Description** This command has no arguments or keywords.

## aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** global configuration command. To disable this feature, use the **no** form of this command.

```
aaa pod server [port port-number] [auth-type {any | all | session-key}] server-key string
```

```
no aaa pod server
```

<b>Syntax Description</b>	<b>port</b> <i>port-number</i>	(Optional) The network access server port to use for packet of disconnect requests. If no port is specified, port 1700 is used.
	<b>auth-type</b>	(Optional) The type of authorization required for disconnecting sessions. If no authentication type is specified, <b>auth-type</b> is the default.
	<b>any</b>	(Optional) Specifies that the session that matches all attributes sent in the POD packet is disconnected. The POD packet can contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
	<b>all</b>	(Optional) Only a session that matches all four key attributes is disconnected. <b>All</b> is the default.
	<b>session-key</b>	(Optional) Specifies that the session that has a matching session-key attribute is disconnected. All other attributes are ignored.
	<b>server-key</b> <i>string</i>	The secret text string that is shared between the network access server and the client workstation. This secret string must be the same on both systems.

## aaa preauth

To enter authentication, authorization, and accounting (AAA) preauthentication configuration mode, use the **aaa preauth** command in global configuration mode. To disable preauthentication, use the **no** form of this command.

**aaa preauth**

**no aaa preauth**

---

**Syntax Description** This command has no arguments or keywords.

## aaa processes

To allocate a specific number of background processes to be used to process authentication, authorization, and accounting (AAA) authentication and authorization requests for PPP, use the **aaa processes** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

**aaa processes** *number*

**no aaa processes** *number*

---

**Syntax Description** *number* Specifies the number of background processes allocated for AAA requests for PPP. Valid entries are 1 to 2147483647.

---

## access-profile

To apply your per-user authorization attributes to an interface during a PPP session, use the **access-profile** command in privileged EXEC mode. Use the default form of the command (no keywords) to cause existing access control lists (ACLs) to be removed and ACLs defined in your per-user configuration to be installed.

**access-profile** [**merge** | **replace**] [**ignore-sanity-checks**]

<b>Syntax Description</b>	<p><b>merge</b> (Optional) Like the default form of the command, this option removes existing ACLs while retaining other existing authorization attributes for the interface.</p> <p>However, using this option also installs per-user authorization attributes in addition to the existing attributes. (The default form of the command installs only new ACLs.) The per-user authorization attributes come from all attribute-value pairs defined in the authentication, authorization, and accounting (AAA) per-user configuration (the user's authorization profile).</p> <p>The resulting authorization attributes of the interface are a combination of the previous and new configurations.</p>
	<p><b>replace</b> (Optional) This option removes existing ACLs <i>and</i> all other existing authorization attributes for the interface.</p> <p>A complete new authorization configuration is then installed, using all AV pairs defined in the AAA per-user configuration.</p> <p>This option is not normally recommended because it initially deletes <i>all</i> existing configurations, including static routes. This could be detrimental if the new user profile does not reinstall appropriate static routes and other critical information.</p>
	<p><b>ignore-sanity-checks</b> (Optional) Enables you to use any AV pairs, whether or not they are valid.</p>

## arap authentication

To enable authentication, authorization, and accounting (AAA) authentication for AppleTalk Remote Access Protocol (ARAP) on a line, use the **arap authentication** command in line configuration mode. To disable authentication for an ARAP line, use the **no** form of the command

```
arap authentication { default | list-name } [one-time]
```

```
no arap authentication { default | list-name }
```



### Caution

If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARAP will be disabled on this line.

<b>Syntax Description</b>	<p><b>default</b> Default list created with the <b>aaa authentication arap</b> command.</p>
	<p><i>list-name</i> Indicated list created with the <b>aaa authentication arap</b> command.</p>
	<p><b>one-time</b> (Optional) Accepts the username and password in the username field.</p>

## clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

**clear ip trigger-authentication**

**Syntax Description** This command has no arguments or keywords.

## dnis

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the **dnis** authentication, authorization, and accounting (AAA) preauthentication configuration command. To remove the **dnis** command from your configuration, use the **no** form of this command.

**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

**no dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

<b>Syntax Description</b>	<b>if-avail</b>	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
	<b>required</b>	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
	<b>accept-stop</b>	(Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element.
	<b>password</b> <i>string</i>	(Optional) Password to use in the Access-Request packet. The default is cisco.

## group

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

**group** {**tacacs+** *server-group*}

**no group** {**tacacs+** *server-group*}

<b>Syntax Description</b>	<b>tacacs+</b>	Uses a TACACS+ server for authentication.
	<i>server-group</i>	Name of the server group to use for authentication.

## ip trigger-authentication (global)

To enable the automated part of double authentication at a device, use the **ip trigger-authentication** command in global configuration mode. To disable the automated part of double authentication, use the **no** form of this command.

**ip trigger-authentication** [*timeout seconds*] [*port number*]

**no ip trigger-authentication**

<b>Syntax Description</b>	<b>timeout</b> <i>seconds</i>	(Optional) Specifies how frequently the local device sends a User Datagram Protocol (UDP) packet to the remote host to request the user's username and password (or PIN). The default is 90 seconds.
	<b>port</b> <i>number</i>	(Optional) Specifies the UDP port to which the local router should send the UPD packet requesting the user's username and password (or PIN). The default is port 7500.

## ip trigger-authentication (interface)

To specify automated double authentication at an interface, use the **ip trigger-authentication** command in interface configuration mode. To turn off automated double authentication at an interface, use the **no** form of this command.

**ip trigger-authentication**

**no ip trigger-authentication**

**Syntax Description** This command has no arguments or keywords.

## isdn guard-timer

To enable a managed timer for authentication requests, use the **isdn guard-timer** interface configuration command. To reset the timer to its default value, use the **no** form of this command.

**isdn guard-timer** *msecs* [**on-expiry** {**accept** | **reject**}]

**no isdn guard-timer**

<b>Syntax Description</b>	<i>msecs</i>	Number of milliseconds that the network access server (NAS) waits for a response from the AAA security server. The valid range is from 1000 through 20,000.
	<b>on-expiry</b>	(Optional) Determines whether calls are accepted or rejected after the specified number of milliseconds has expired. If no expiry action is selected, calls are rejected.

<b>accept</b>	(Optional) Calls are accepted if the guard-timer expires before AAA responds.
<b>reject</b>	(Optional) Calls are rejected if the guard-timer expires before AAA responds.

## login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication** command in line configuration mode. To return to the default specified by the **aaa authentication login** command, use the **no** form of this command.

```
login authentication { default | list-name }
```

```
no login authentication { default | list-name }
```

### Syntax Description

<b>default</b>	Uses the default list created with the <b>aaa authentication login</b> command.
<i>list-name</i>	Uses the indicated list created with the <b>aaa authentication login</b> command.

## nasi authentication

To enable authentication, authorization, and accounting (AAA) authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** command in line configuration mode. To return to the default, as specified by the **aaa authentication nasi** command, use the **no** form of the command.

```
nasi authentication { default | list-name }
```

```
no nasi authentication { default | list-name }
```

### Syntax Description

<b>default</b>	Uses the default list created with the <b>aaa authentication nasi</b> command.
<i>list-name</i>	Uses the list created with the <b>aaa authentication nasi</b> command.

## ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and to specify the order in which CHAP and PAP authentication are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

```
ppp authentication {protocol1 [protocol2...] [if-needed] [list-name | default] [callin]  
[one-time]}
```

```
no ppp authentication
```

<b>Syntax Description</b>	<i>protocol1</i> [ <i>protocol2...</i> ]	Specify at least one of the keywords described in Table 23.
	<b>if-needed</b>	(Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
	<i>list-name</i>	(Optional) Used with AAA. Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the <b>aaa authentication ppp</b> command.
	<b>default</b>	(Optional) The name of the method list is created with the <b>aaa authentication ppp</b> command.
	<b>callin</b>	(Optional) Specifies authentication on incoming (received) calls only.
	<b>one-time</b>	(Optional) Accepts the username and password in the username field.

**Table 23**  *ppp authentication Protocols*

<b>chap</b>	Enables CHAP on a serial interface.
<b>ms-chap</b>	Enables Microsoft's version of CHAP (MS-CHAP) on a serial interface.
<b>pap</b>	Enables PAP on a serial interface.

## ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with Challenge Handshake Authentication Protocol (CHAP), use the **ppp chap hostname** command in interface configuration mode. To disable this function, use the **no** form of the command.

**ppp chap hostname** *hostname*

**no ppp chap hostname** *hostname*

<b>Syntax Description</b>	<i>hostname</i>	The name sent in the CHAP challenge.
---------------------------	-----------------	--------------------------------------

## ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password to use in response to challenges from an unknown peer, use the **ppp chap password** command in interface configuration mode. To disable the PPP CHAP password, use the **no** form of this command.

**ppp chap password** *secret*

**no ppp chap password** *secret*

<b>Syntax Description</b>	<i>secret</i>	The secret used to compute the response value for any CHAP challenge from an unknown peer.
---------------------------	---------------	--

## ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

**ppp chap refuse** [*callin*]

**no ppp chap refuse** [*callin*]

<b>Syntax Description</b>	<b>callin</b>	(Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.
---------------------------	---------------	--

## ppp chap wait

To specify that the router will not authenticate to a peer requesting Challenge Handshake Authentication Protocol (CHAP) authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** command in interface configuration mode. To allow the router to respond immediately to an authentication challenge, use the **no** form of this command.

**ppp chap wait** *secret*

**no ppp chap wait** *secret*

<b>Syntax Description</b>	<i>secret</i>	The secret used to compute the response value for any CHAP challenge from an unknown peer.
---------------------------	---------------	--

## ppp pap

To refuse a peer request to authenticate remotely with PPP using Password Authentication Protocol, use the **ppp pap** interface configuration command. To disable the refusal, use the **no** form of this command.

**ppp pap refuse**

**no ppp pap refuse**

<b>Syntax Description</b>	<b>refuse</b>	Signifies that authentication using PAP is denied.
---------------------------	---------------	--

## ppp pap sent-username

To reenable remote Password Authentication Protocol (PAP) support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

```
ppp pap sent-username username password password
```

```
no ppp pap sent-username
```

---

**Syntax Description**

<i>username</i>	Username sent in the PAP authentication request.
<b>password</b>	Password sent in the PAP authentication request.
<i>password</i>	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

---

## show ip trigger-authentication

To view the list of remote hosts for which automated double authentication has been attempted, use the **show ip trigger-authentication** command in privileged EXEC mode.

```
show ip trigger-authentication
```

---

**Syntax Description**

This command has no arguments or keywords.

## show ppp queues

To monitor the number of requests processed by each authentication, authorization, and accounting (AAA) background process, use the **show ppp queues** command in privileged EXEC mode.

```
show ppp queues
```

---

**Syntax Description**

This command has no arguments or keywords.

# timeout login response

To specify how long the system will wait for login input (such as username and password) before timing out, use the **timeout login response** command in line configuration mode. To set the timeout value to 0 seconds, use the **no** form of this command.

**timeout login response** *seconds*

**no timeout login response** *seconds*

---

**Syntax Description**

---

*seconds*

Integer that determines the number of seconds the system will wait for login input before timing out. Available settings are from 1 to 300 seconds.

---



## Authorization Commands

This chapter describes the function and syntax of the authorization commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### aaa authorization

To set parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To disable authorization for a function, use the **no** form of this command.

```
aaa authorization { network | exec | commands level | reverse-access | configuration } { default | list-name } method1 [method2...]
```

```
no aaa authorization { network | exec | commands level | reverse-access | configuration | default | list-name }
```

#### Syntax Description

<b>network</b>	Runs authorization for all network-related service requests, including SLIP <sup>1</sup> , PPP <sup>2</sup> , PPP NCPs <sup>3</sup> , and ARA <sup>4</sup> .
<b>exec</b>	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as <b>autocommand</b> information.
<b>commands</b>	Runs authorization for all commands at the specified privilege level.
<i>level</i>	Specific command level that should be authorized. Valid entries are 0 through 15.
<b>reverse-access</b>	Runs authorization for reverse access connections, such as reverse Telnet.
<b>configuration</b>	Downloads the configuration from the AAA server.
<b>default</b>	Uses the listed authorization methods that follow this argument as the default list of methods for authorization.
<i>list-name</i>	Character string used to name the list of authorization methods.
<i>method1</i> [ <i>method2...</i> ]	One of the keywords listed in Table 24.

1. Serial Line Internet Protocol
2. Point-to-Point Protocol
3. Point-to-Point Protocol Network Control Programs
4. AppleTalk Remote Access

Table 24 *aaa authorization Methods*

Keyword	Description
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> command.
<b>if-authenticated</b>	Allows the user to access the requested function if the user is authenticated.
<b>krb5-instance</b>	Uses the instance defined by the <b>kerberos instance map</b> command.
<b>local</b>	Uses the local database for authorization.
<b>none</b>	No authorization is performed.

## aaa authorization config-commands

To reestablish the default created when the **aaa authorization commands** command was issued, use the **aaa authorization config-commands** command in global configuration mode. To disable authentication, authorization, and accounting (AAA) configuration command authorization, use the **no** form of this command.

**aaa authorization config-commands**

**no aaa authorization config-commands**

**Syntax Description** This command has no arguments or keywords.

## aaa authorization reverse-access

To configure a network access server to request authorization information from a security server before allowing a user to establish a reverse Telnet session, use the **aaa authorization reverse-access** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

**aaa authorization reverse-access {group radius | group tacacs+}**

**no aaa authorization reverse-access {group radius | group tacacs+}**

Syntax Description	
<b>group radius</b>	Specifies that the network access server will request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session.
<b>group tacacs+</b>	Specifies that the network access server will request authorization from a TACACS+ security server before allowing a user to establish a reverse Telnet session.

## aaa dnis map authorization network group

To map a Dialed Number Identification Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group (the server group that will be used for AAA authorization), use the **aaa dnis map authorization network group** global configuration command. To unmap this DNIS number from the defined server group, use the **no** form of this command.

```
aaa dnis map dnis-number authorization network group server-group-name
```

```
no aaa dnis map dnis-number authorization network group server-group-name
```

### Syntax Description

<i>dnis-number</i>	Number of the DNIS.
<i>server-group-name</i>	Character string used to name a group of security servers functioning within a server group.

## authorization

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line configuration mode. To disable authorization, use the **no** form of this command.

```
authorization {arap | commands level | exec | reverse-access} [default | list-name]
```

```
no authorization {arap | commands level | exec | reverse-access} [default | list-name]
```

### Syntax Description

<b>arap</b>	Enables authorization for lines configured for AppleTalk Remote Access (ARA) protocol.
<b>commands</b>	Enables authorization on the selected lines for all commands at the specified privilege level.
<i>level</i>	Specific command level to be authorized. Valid entries are 0 through 15.
<b>exec</b>	Enables authorization to determine if the user is allowed to run an EXEC shell on the selected lines.
<b>reverse-access</b>	Enables authorization to determine if the user is allowed reverse access privileges.
<b>default</b>	(Optional) The name of the default method list, created with the <b>aaa authorization</b> command.
<i>list-name</i>	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the <b>aaa authorization</b> command.

# ppp authorization

To enable authentication, authorization, and accounting (AAA) authorization on the selected interface, use the **ppp authorization** command in interface configuration mode. To disable authorization, use the **no** form of this command.

**ppp authorization** [**default** | *list-name*]

**no ppp authorization**

---

## Syntax Description

---

<b>default</b>	(Optional) The name of the method list is created with the <b>aaa authorization</b> command.
<i>list-name</i>	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the <b>aaa authorization</b> command.

---



# Accounting Commands

---

This chapter describes the function and syntax of the accounting commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

## aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

```
aaa accounting { auth-proxy | system | network | exec | connection | commands level } { default | list-name } { start-stop | stop-only | wait-start | none } [broadcast] group groupname
```

```
no aaa accounting { auth-proxy | system | network | exec | connection | commands level } { default | list-name } [broadcast] group groupname
```

<b>auth-proxy</b>	Provides information about all authenticated-proxy user events.
<b>system</b>	Performs accounting for all system-level events not associated with users, such as reloads.
<b>network</b>	Runs accounting for all network-related service requests, including SLIP <sup>1</sup> , PPP <sup>2</sup> , PPP NCPs <sup>3</sup> , and ARAP <sup>4</sup> .
<b>exec</b>	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the <b>autocommand</b> command.
<b>connection</b>	Provides information about all outbound connections made from the network access server, such as Telnet, LAT <sup>5</sup> , TN3270, PAD <sup>6</sup> , and rlogin.
<b>commands level</b>	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
<b>default</b>	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
<i>list-name</i>	Character string used to name the list of at least one of the accounting methods described in Table 25.

<b>start-stop</b>	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
<b>stop-only</b>	Sends a “stop” accounting notice at the end of the requested user process.
<b>wait-start</b>	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process does not begin until the “start” accounting notice is received by the server.
<b>none</b>	Disables accounting services on this line or interface.
<b>broadcast</b>	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.
<b>group <i>groupname</i></b>	At least one of the keywords described in Table 26.

1. SLIP = Serial Line Internet Protocol
2. PPP = Point-to-Point Protocol
3. PPP NCPs = Point-to-Point Protocol Network Control Protocols
4. ARAP = AppleTalk Remote Access Protocol
5. LAT = local-area transport
6. PAD = packet assembler/disassembler

**Table 25** *aaa accounting Methods Lists*

<b>Keyword</b>	<b>Description</b>
<b>auth-proxy</b>	Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service.
<b>commands</b>	Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level.
<b>connection</b>	Creates a method list to provide accounting information about all outbound connections made from the network access server.
<b>exec</b>	Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.
<b>network</b>	Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARA sessions.
<b>resource</b>	Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated.

Table 26 *aaa accounting Methods*

Keyword	Description
<b>group radius</b>	Uses the list of all RADIUS servers for authentication as defined by the <b>aaa group server radius</b> command.
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication as defined by the <b>aaa group server tacacs+</b> command.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> .

## aaa accounting connection h323

To define the accounting method list H.323 with RADIUS as a method with either **stop-only** or **start-stop** accounting options, use the **aaa accounting connection h323** command in global configuration mode. To disable the use of this accounting method list, use the **no** form of this command.

```
aaa accounting connection h323 {stop-only | start-stop | wait-start | none} [broadcast] group
groupname
```

```
no aaa accounting connection h323 {stop-only | start-stop | wait-start | none} [broadcast]
group groupname
```

Syntax Description	
<b>stop-only</b>	Sends a “stop” accounting notice at the end of the requested user process.
<b>start-stop</b>	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
<b>wait-start</b>	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process does not begin until the “start” accounting notice is received by the server.
<b>none</b>	Disables accounting services on this line or interface.
<b>broadcast</b>	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
<b>group</b> <i>groupname</i>	Specifies the server group to be used for accounting services. The following are valid server group names: <ul style="list-style-type: none"> <li>• <i>string</i>: Character string used to name a server group.</li> <li>• <b>radius</b>: Uses list of all RADIUS hosts.</li> <li>• <b>tacacs+</b>: Uses list of all TACACS+ hosts.</li> </ul>

## aaa accounting nested

To specify that NETWORK records be generated, or nested, within EXEC “start” and “stop” records for PPP users who start EXEC terminal sessions, use the **aaa accounting nested** command in global configuration mode. To allow the sending of records for users with a NULL username, use the **no** form of this command.

**aaa accounting nested**

**no aaa accounting nested**

**Syntax Description** This command has no arguments or keywords.

## aaa accounting resource start-stop group

To enable full resource accounting, which will generate both a “start” record at call setup and a “stop” record at call termination, use the **aaa accounting resource start-stop group** command in global configuration mode. To disable full resource accounting, use the **no** form of this command.

**aaa accounting resource** *method-list* **start-stop** [**broadcast**] **group** *groupname*

**no aaa accounting resource** *method-list* **start-stop** [**broadcast**] **group** *groupname*

<b>Syntax Description</b>	<i>method-list</i>	Method used for accounting services. Use one of the following options: <ul style="list-style-type: none"> <li><b>default</b>: Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.</li> <li><i>string</i>: Character string used to name the list of accounting methods.</li> </ul>
	<b>broadcast</b>	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
	<b>group</b> <i>groupname</i>	Specifies the server group to be used for accounting services. The following are valid server group names: <ul style="list-style-type: none"> <li><i>string</i>: Character string used to name a server group.</li> <li><b>radius</b>: Uses list of all RADIUS hosts.</li> <li><b>tacacs+</b>: Uses list of all TACACS+ hosts.</li> </ul>

## aaa accounting resource stop-failure group

To enable resource failure stop accounting support, which will generate a “stop” record at any point prior to user authentication only if a call is terminated, use the **aaa accounting resource stop-failure group** command in global configuration mode. To disable resource failure stop accounting, use the **no** form of this command.

```
aaa accounting resource method-list stop-failure [broadcast] group groupname
```

```
no aaa accounting resource method-list stop-failure [broadcast] group groupname
```

Syntax Description		
	<i>method-list</i>	Method used for accounting services. Use one of the following options: <ul style="list-style-type: none"> <li>• <b>default</b>: Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.</li> <li>• <i>string</i>: Character string used to name the list of accounting methods.</li> </ul>
	<b>broadcast</b>	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
	<b>group</b> <i>groupname</i>	Group to be used for accounting services. Use one of the following options: <ul style="list-style-type: none"> <li>• <i>string</i>: Character string used to name a server group.</li> <li>• <b>radius</b>: Uses list of all RADIUS hosts.</li> <li>• <b>tacacs+</b>: Uses list of all TACACS+ hosts.</li> </ul>

## aaa accounting send stop-record authentication failure

To generate accounting “stop” records for users who fail to authenticate at login or during session negotiation, use the **aaa accounting send stop-record authentication failure** command in global configuration mode. To stop generating records for users who fail to authenticate at login or during session negotiation, use the **no** form of this command.

```
aaa accounting send stop-record authentication failure
```

```
no aaa accounting send stop-record authentication failure
```

Syntax Description	
	This command has no arguments or keywords.

## aaa accounting suppress null-username

To prevent the Cisco IOS software from sending accounting records for users whose username string is NULL, use the **aaa accounting suppress null-username** command in global configuration mode. To allow sending records for users with a NULL username, use the **no** form of this command.

```
aaa accounting suppress null-username
```

```
no aaa accounting suppress null-username
```

**Syntax Description** This command has no arguments or keywords.

## aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update** command in global configuration mode. To disable interim accounting updates, use the **no** form of this command.

```
aaa accounting update [newinfo] [periodic number]
```

```
no aaa accounting update
```

<b>Syntax Description</b>	<b>newinfo</b>	(Optional) Causes an interim accounting record to be sent to the accounting server whenever there is new accounting information to report relating to the user in question.
	<b>periodic</b>	(Optional) Causes an interim accounting record to be sent to the accounting server periodically, as defined by the argument <i>number</i> .
	<i>number</i>	Integer specifying number of minutes.

## aaa dnis map accounting network

To map a Dialed Number Information Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group that will be used for AAA accounting, use the **aaa dnis map accounting network** command in global configuration mode. To remove DNIS mapping from the named server group, use the **no** form of this command.

```
aaa dnis map dnis-number accounting network [start-stop | stop-only | wait-start | none]
[broadcast] group groupname
```

```
no aaa dnis map dnis-number accounting network
```

Syntax Description		
	<i>dnis-number</i>	Number of the DNIS.
	<b>start-stop</b>	(Optional) Indicates that the defined security server group will send a “start accounting” notice at the beginning of a process and a “stop accounting” notice at the end of a process. The “start accounting” record is sent in the background. (The requested user process begins regardless of whether the “start accounting” notice was received by the accounting server.)
	<b>stop-only</b>	(Optional) Indicates that the defined security server group will send a “stop accounting” notice at the end of the requested user process.
	<b>wait-start</b>	(Optional) Sends a “start accounting” notice at the beginning of a process and a “stop accounting” notice at the end of a process. The “start accounting” record is sent in the background. The requested user process does not begin until the “start accounting” notice is received by the server.
	<b>none</b>	(Optional) Indicates that the defined security server group will not send accounting notices.
	<b>broadcast</b>	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
	<b>group</b> <i>groupname</i>	At least one of the keywords described in Table 27.

**Table 27 AAA Accounting Methods**

Keyword	Description
<b>group radius</b>	Uses the list of all RADIUS servers for authentication as defined by the <b>aaa group server radius</b> command.
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication as defined by the <b>aaa group server tacacs+</b> command.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> .

## aaa session-mib

To enable disconnect by using Simple Network Management Protocol (SNMP), use the **aaa session-mib** global configuration mode command. To disable this function, use the **no** form of this command.

**aaa session-mib disconnect**

**no aaa session-mib disconnect**

Syntax Description		
	<b>disconnect</b>	Enables authentication, authorization, and accounting (AAA) session MIB disconnect.

## accounting

To enable authentication, authorization, and accounting (AAA) accounting services to a specific line or group of lines, use the **accounting** command in line configuration mode. To disable AAA accounting services, use the **no** form of this command.

**accounting** { **arap** | **commands** *level* | **connection** | **exec** } [**default** | *list-name*]

**no accounting** { **arap** | **commands** *level* | **connection** | **exec** } [**default** | *list-name*]

### Syntax Description

<b>arap</b>	Enables accounting on lines configured for AppleTalk Remote Access Protocol (ARAP).
<b>commands</b> <i>level</i>	Enables accounting on the selected lines for all commands at the specified privilege level. Valid privilege level entries are 0 through 15.
<b>connection</b>	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
<b>exec</b>	Enables accounting for all system-level events not associated with users, such as reloads on the selected lines.
<b>default</b>	(Optional) The name of the default method list, created with the <b>aaa accounting</b> command.
<i>list-name</i>	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the <b>aaa accounting</b> command.

## accounting (gatekeeper)

To enable the accounting on the gatekeeper, use the **accounting** command in gatekeeper configuration mode. To disable accounting, use the **no** form of this command.

**accounting**

**no accounting**

### Syntax Description

This command has no arguments or keywords.

## ppp accounting

To enable authentication, authorization, and accounting (AAA) accounting services on the selected interface, use the **ppp accounting** command in interface configuration mode. To disable AAA accounting services, use the **no** form of this command.

**ppp accounting default**

**no ppp accounting**

---

**Syntax Description**

---

<b>default</b>	The name of the method list is created with the <b>aaa accounting</b> command.
----------------	--

---

## show accounting

To step through all active sessions and to print all the accounting records for actively accounted functions, use the **show accounting** command in EXEC mode. Use the **no** form of this command to disable viewing and printing accounting records.

**show accounting**

**no show accounting**

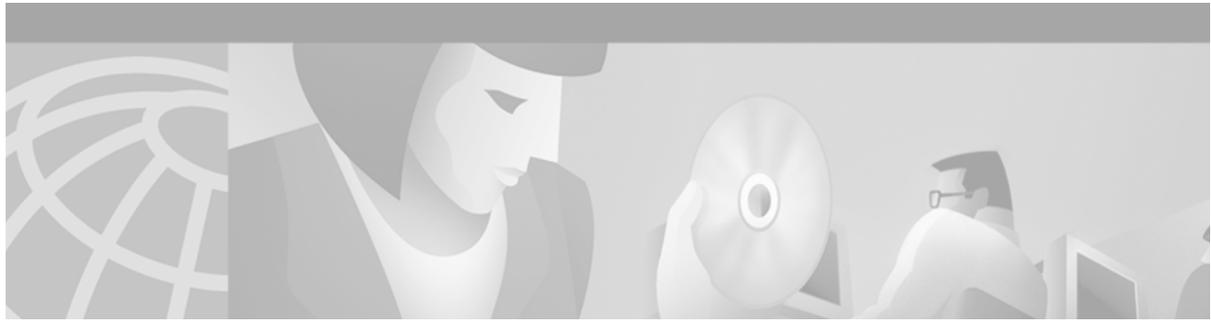
---

**Syntax Description**

---

This command has no arguments or keywords.





## RADIUS Commands

---

This chapter describes the function and syntax of the RADIUS commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

```
aaa group server radius group-name
```

```
no aaa group server radius group-name
```

---

**Syntax Description**

*group-name*

Character string used to name the group of servers.

---

### aaa nas port extended

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the **aaa nas port extended** command in global configuration mode. To display no extended field information, use the **no** form of this command.

```
aaa nas port extended
```

```
no aaa nas port extended
```

---

**Syntax Description**

This command has no arguments or keywords.

## call guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **call guard-timer** controller configuration command. To remove the **call guard-timer** command from your configuration file, use the **no** form of this command.

```
call guard-timer milliseconds [on-expiry {accept | reject}]
```

```
no call guard-timer milliseconds [on-expiry {accept | reject}]
```

<b>Syntax Description</b>	<i>milliseconds</i>	Specifies the number of milliseconds to wait for a response from the RADIUS server.
	<b>on-expiry accept</b>	(Optional) Accepts the call if a response is not received from the RADIUS server within the specified time.
	<b>on-expiry reject</b>	(Optional) Rejects the call if a response is not received from the RADIUS server within the specified time.

## clid

To preauthenticate calls on the basis of the Calling Line Identification (CLID) number, use the **clid** authentication, authorization, and accounting (AAA) preauthentication configuration command. To remove the **clid** command from your configuration, use the **no** form of this command.

```
clid [if-avail | required] [accept-stop] [password password]
```

```
no clid [if-avail | required] [accept-stop] [password password]
```

<b>Syntax Description</b>	<b>if-avail</b>	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
	<b>required</b>	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
	<b>accept-stop</b>	(Optional) Prevents subsequent preauthentication elements such as <b>ctype</b> or <b>dnis</b> from being tried once preauthentication has succeeded for a call element.
	<b>password</b> <i>password</i>	(Optional) Defines the password for the preauthentication element.

# ctype

To preauthenticate calls on the basis of the call type, use the **ctype** authentication, authorization, and accounting (AAA) preauthentication configuration command. To remove the **ctype** command from your configuration, use the **no** form of this command.

**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

**no ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

Syntax Description		
<b>if-avail</b>	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.	
<b>required</b>	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.	
<b>accept-stop</b>	(Optional) Prevents subsequent preauthentication elements such as <b>clid</b> or <b>dnis</b> from being tried once preauthentication has succeeded for a call element.	
<b>password</b> <i>password</i>	(Optional) Defines the password for the preauthentication element.	
<b>digital</b>	(Optional) Specifies “digital” as the call type for preauthentication.	
<b>speech</b>	(Optional) Specifies “speech” as the call type for preauthentication.	
<b>v.110</b>	(Optional) Specifies “v.110” as the call type for preauthentication.	
<b>v.120</b>	(Optional) Specifies “v.120” as the call type for preauthentication.	

## deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the **deadtime** server group configuration command. To set deadtime to 0, use the **no** form of this command.

**deadtime** *minutes*

**no deadtime**

Syntax Description		
<i>minutes</i>	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).	

## dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of this command.

**dialer aaa suffix** *string* **password** *string*

**no dialer aaa password suffix** *string* **password** *string*

### Syntax Description

<b>suffix</b> <i>string</i>	Defines a suffix for authentication.
<b>password</b> <i>string</i>	Defines a nondefault password for authentication.

## dnis (AAA preauthentication configuration)

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the **dnis** AAA preauthentication configuration command. To remove the **dnis** command from your configuration, use the **no** form of this command.

**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

**no dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *password*]

### Syntax Description

<b>if-avail</b>	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
<b>required</b>	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
<b>accept-stop</b>	(Optional) Prevents subsequent preauthentication elements such as <b>clid</b> or <b>ctype</b> from being tried once preauthentication has succeeded for a call element.
<b>password</b> <i>password</i>	(Optional) Defines the password for the preauthentication element.

## dnis bypass (AAA preauthentication configuration)

To specify a group of DNIS (Dial Number Identification Service) numbers that will be bypassed for preauthentication, use the **dnis bypass** AAA preauthentication configuration command. To remove the **dnis bypass** command from your configuration, use the **no** form of this command.

```
dnis bypass {dnis-group-name}
```

```
no dnis bypass {dnis-group-name}
```

---

**Syntax Description**

---

<i>dnis-group-name</i>	Name of the defined DNIS group.
------------------------	---------------------------------

---

## group (AAA preauthentication configuration)

To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the **group** AAA preauthentication configuration command. To remove the **group** command from your configuration, use the **no** form of this command.

```
group server-group
```

```
no group server-group
```

---

**Syntax Description**

---

<i>server-group</i>	Specifies a AAA RADIUS server group.
---------------------	--------------------------------------

---

## ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the **no** form of this command.

```
ip radius source-interface subinterface-name
```

```
no ip radius source-interface
```

---

**Syntax Description**

---

<i>subinterface-name</i>	Name of the interface that RADIUS uses for all of its outgoing packets.
--------------------------	---

---

## isdn guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **isdn guard-timer** interface configuration command. To remove the **isdn guard-timer** command from your configuration file, use the **no** form of this command.

```
isdn guard-timer milliseconds [on-expiry {accept | reject}]
```

```
no isdn guard-timer milliseconds [on-expiry {accept | reject}]
```

<b>Syntax Description</b>	<i>milliseconds</i>	Specifies the number of milliseconds to wait for a response from the RADIUS server.
	<b>on-expiry accept</b>	(Optional) Accepts the call if a response is not received from the RADIUS server within the specified time.
	<b>on-expiry reject</b>	(Optional) Rejects the call if a response is not received from the RADIUS server within the specified time.

## radius-server attribute 8 include-in-access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include-in-access-req** global configuration command. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

```
radius-server attribute 8 include-in-access-req
```

```
no radius-server attribute 8 include-in-access-req
```

**Syntax Description** This command has no arguments or keywords.

## radius-server attribute 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in the access request, use the **radius-server attribute 32 include-in-access-req** global configuration command. To disable sending RADIUS attribute 32 in the access-request, use the **no** form of this command.

```
radius-server attribute 32 include-in-access-req [format]
```

```
no radius-server attribute 32 include-in-access-req
```

**Syntax Description**

<i>format</i>	(Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), and a domain name (%d).
---------------	--

## radius-server attribute 44 include-in-access-req

To send RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication), use the **radius-server attribute 44 include-in-access-req** global configuration command. To remove this command from your configuration, use the **no** form of this command.

```
radius-server attribute 44 include-in-access-req
```

```
no radius-server attribute 44 include-in-access-req
```

**Syntax Description** This command has no arguments or keywords.

## radius-server attribute 69 clear

To receive nonencrypted tunnel passwords in attribute 69 (Tunnel-Password), use the **radius-server attribute 69 clear** global configuration command. To disable this feature and receive encrypted tunnel passwords, use the **no** form of this command.

```
radius-server attribute 69 clear
```

```
no radius-server attribute 69 clear
```

**Syntax Description** This command has no arguments or keywords.

## radius-server attribute 188 format non-standard

To send the number of remaining links in the multilink bundle in the accounting-request packet, use the **radius-server attribute 188 format non-standard** global configuration command. To disable the sending of the number of links in the multilink bundle in the accounting-request packet, use the **no** form of this command.

```
radius-server attribute 188 format non-standard
```

```
no radius-server attribute 188 format non-standard
```

**Syntax Description** This command has no arguments or keywords.

## radius-server attribute nas-port extended

The **radius-server attribute nas-port extended** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command in this chapter for more information.

## radius-server attribute nas-port format

To select the NAS-Port format used for RADIUS accounting features, use the **radius-server attribute nas-port format** global configuration command. To restore the default NAS-Port format, use the **no** form of this command.

**radius-server attribute nas-port format** *format*

**no radius-server attribute nas-port format** *format*

<b>Syntax Description</b>	<i>format</i>	NAS-Port format. Possible values for the <i>format</i> argument are as follows: <ul style="list-style-type: none"> <li><b>a</b>—Standard NAS-Port format</li> <li><b>b</b>—Extended NAS-Port format</li> <li><b>c</b>—Shelf-slot NAS-Port format</li> <li><b>d</b>—PPP extended NAS-Port format</li> </ul>
---------------------------	---------------	--

## radius-server challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the **radius-server challenge-noecho** global configuration command. To return to the default condition, use the **no** form of this command.

**radius-server challenge-noecho**

**no radius-server challenge-noecho**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## radius-server configure-nas

To have the Cisco router or access server query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up, use the **radius-server configure-nas** command in global configuration mode. To discontinue the query of the RADIUS server, use the **no** form of this command.

**radius-server configure-nas**

**no radius-server configure-nas**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## radius-server deadtime

To improve RADIUS response times when some servers might be unavailable, use the **radius-server deadtime** command in global configuration mode to cause the unavailable servers to be skipped immediately. To set dead-time to 0, use the **no** form of this command.

**radius-server deadtime** *minutes*

**no radius-server deadtime**

<b>Syntax Description</b>	<i>minutes</i>	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).
---------------------------	----------------	--

## radius-server directed-request

To allow users logging into a Cisco network access server (NAS) to select a RADIUS server for authentication, use the **radius-server directed-request** global configuration command. To disable the directed-request feature, use the **no** form of this command.

**radius-server directed-request** [*restricted*]

**no radius-server directed-request** [*restricted*]

<b>Syntax Description</b>	<i>restricted</i>	(Optional) Prevents the user from being sent to a secondary server if the specified server is not available.
---------------------------	-------------------	--

## radius-server extended-portnames

The **radius-server extended-portnames** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command in this chapter for more information.

## radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}]

**no radius-server host** {*hostname* | *ip-address*}

Syntax Description	
<i>hostname</i>	Domain Name System (DNS) name of the RADIUS server host.
<i>ip-address</i>	IP address of the RADIUS server host.
<b>auth-port</b>	(Optional) Specifies the UDP destination port for authentication requests.
<i>port-number</i>	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
<b>acct-port</b>	(Optional) Specifies the UDP destination port for accounting requests.
<i>port-number</i>	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
<b>timeout</b>	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the <b>radius-server timeout</b> command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
<i>seconds</i>	(Optional) Specifies the <b>timeout</b> value. Enter a value in the range 1 to 1000. If no <b>timeout</b> value is specified, the global value is used.
<b>retransmit</b>	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the <b>radius-server retransmit</b> command.
<i>retries</i>	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.
<b>key</b>	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the <b>radius-server key</b> command. If no key string is specified, the global value is used.  The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the <b>radius-server host</b> command syntax. This is because the 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 themselves are part of the key.
<i>string</i>	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
<b>alias</b>	(Optional) Allows up to eight aliases per line for any given RADIUS server.

## radius-server host non-standard

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command in global configuration mode. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

```
radius-server host {hostname | ip-address} non-standard
```

```
no radius-server host {hostname | ip-address} non-standard
```

<b>Syntax Description</b>	<i>hostname</i>	DNS name of the RADIUS server host.
	<i>ip-address</i>	IP address of the RADIUS server host.

## radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

```
radius-server key {0 string | 7 string | string}
```

```
no radius-server key
```

<b>Syntax Description</b>	<b>0</b>	Specifies that an unencrypted key will follow.
	<i>string</i>	The unencrypted (cleartext) shared key.
	<b>7</b>	Specifies that a hidden key will follow.
	<i>string</i>	The hidden shared key.
	<i>string</i>	The unencrypted (cleartext) shared key.

## radius-server optional passwords

To specify that the first RADIUS request to a RADIUS server be made *without* password verification, use the **radius-server optional-passwords** command in global configuration mode. To restore the default, use the **no** form of this command.

```
radius-server optional-passwords
```

```
no radius-server optional-passwords
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up, use the **radius-server retransmit** command in global configuration mode. To disable retransmission, use the **no** form of this command.

```
radius-server retransmit retries
```

```
no radius-server retransmit
```

<b>Syntax Description</b>	<i>retries</i>	Maximum number of retransmission attempts. The default is 3 attempts.
---------------------------	----------------	---

## radius-server timeout

To set the interval for which a router waits for a server host to reply, use the **radius-server timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

**radius-server timeout** *seconds*

**no radius-server timeout**

Syntax Description	<i>seconds</i>	Number that specifies the timeout interval, in seconds. The default is 5 seconds.
--------------------	----------------	---

## radius-server vsa send

To configure the network access server to recognize and use vendor-specific attributes, use the **radius-server vsa send** command in global configuration mode. To restore the default, use the **no** form of this command.

**radius-server vsa send** [**accounting** | **authentication**]

**no radius-server vsa send** [**accounting** | **authentication**]

Syntax Description	<b>accounting</b>	(Optional) Limits the set of recognized vendor-specific attributes to only accounting attributes.
	<b>authentication</b>	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

## server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server** command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

**no server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description	<i>ip-address</i>	IP address of the RADIUS server host.
	<b>auth-port</b> <i>port-number</i>	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The port-number argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.
	<b>acct-port</b> <i>port-number</i>	(Optional) Specifies the UDP destination port for accounting requests. The port number argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.

## show radius statistics

To display the RADIUS statistics for accounting and authentication packets, use the **show radius statistics** EXEC command.

```
show radius statistics
```

---

**Syntax Description** This command has no arguments or keywords.

## vpdn aaa attribute nas-port vpdn-nas

To enable the L2TP network server (LNS) to send PPP extended NAS-Port format values from the L2TP access concentrator (LAC) to the RADIUS server for accounting, use the **vpdn aaa attribute nas-port vpdn-nas** global configuration command. To prevent the LNS from sending PPP extended NAS-Port format values, use the **no** form of this command.

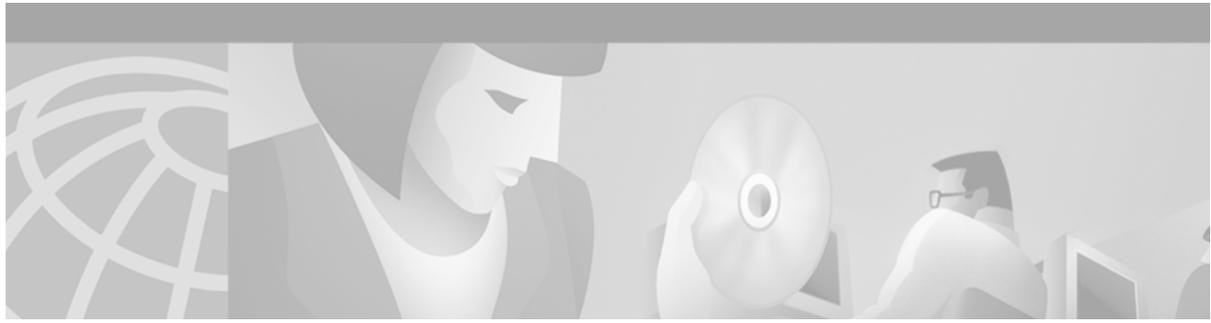
```
vpdn aaa attribute nas-port vpdn-nas
```

```
no vpdn aaa attribute nas-port vpdn-nas
```

---

**Syntax Description** This command has no arguments or keywords.

■ vpdn aaa attribute nas-port vpdn-nas



## TACACS+ Commands

---

This chapter describes the function and syntax of the TACACS+ commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### aaa group server tacacs+

To group different server hosts into distinct lists and distinct methods, use the **aaa group server tacacs+** command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

**aaa group server tacacs+** *group-name*

**no aaa group server tacacs+** *group-name*

<b>Syntax Description</b>	<b>tacacs+</b>	Uses only the TACACS+ server hosts.
	<i>group-name</i>	Character string used to name the group of servers.

### ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

**ip tacacs source-interface** *subinterface-name*

**no ip tacacs source-interface**

<b>Syntax Description</b>	<i>subinterface-name</i>	Name of the interface that TACACS+ uses for all of its outgoing packets.
---------------------------	--------------------------	--

## server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

**server** *ip-address*

**no server** *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the selected server.
--------------------	-------------------	------------------------------------

## tacacs-server directed-request

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request** command in global configuration mode. To send the entire string to the TACACS+ server, use the **no** form of this command.

**tacacs-server directed-request** [**restricted**] [**no-truncate**]

**no tacacs-server directed-request**

Syntax Description	<b>restricted</b>	(Optional) Restrict queries to directed request servers only.
	<b>no-truncate</b>	(Optional) Do not truncate the @hostname from the username.

## tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no** form of this command.

**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]

**no tacacs-server host** *hostname*

Syntax Description	<i>hostname</i>	Name or IP address of the host.
	<b>port</b>	(Optional) Specify a server port number. This option overrides the default, which is port 49.
	<i>integer</i>	(Optional) Port number of the server. Valid port numbers range from 1 to 65535.
	<b>timeout</b>	(Optional) Specify a timeout value. This overrides the global timeout value set with the <b>tacacs-server timeout</b> command for this server only.
	<i>integer</i>	(Optional) Integer value, in seconds, of the timeout interval.

---

<b>key</b>	(Optional) Specify an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command <b>tacacs-server key</b> for this server only.
<i>string</i>	(Optional) Character string specifying authentication and encryption key.

---

## tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the **tacacs-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

**tacacs-server key** *key*

**no tacacs-server key** [*key*]

---

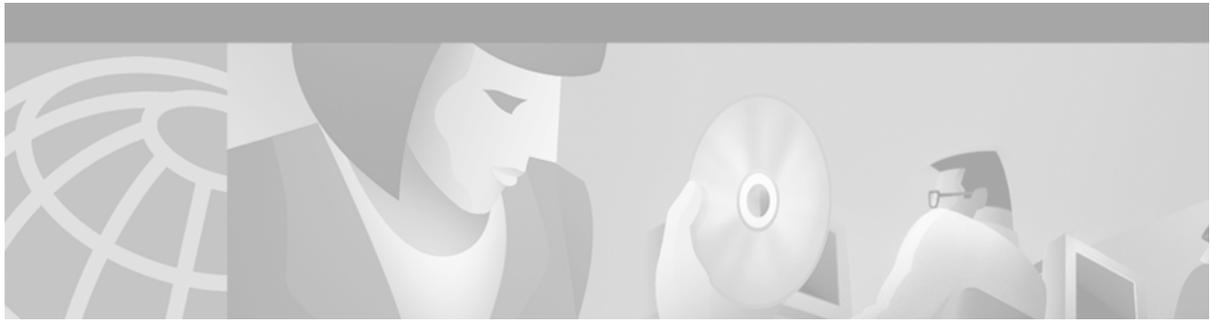
### Syntax Description

---

<i>key</i>	Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.
------------	--

---





## Kerberos Commands

---

This chapter describes the function and syntax of the Kerberos commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** command in privileged EXEC mode.

**clear kerberos creds**

---

**Syntax Description** This command has no arguments or keywords.

### kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** command in global configuration mode. To make Kerberos optional, use the **no** form of this command.

**kerberos clients mandatory**

**no kerberos clients mandatory**

---

**Syntax Description** This command has no arguments or keywords.

## kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** command in global configuration mode. To turn off forwarding of Kerberos credentials, use the **no** form of this command.

**kerberos credentials forward**

**no kerberos credentials forward**

**Syntax Description** This command has no arguments or keywords.

## kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** command in global configuration mode. To remove a Kerberos instance map, use the **no** form of this command.

**kerberos instance map** *instance privilege-level*

**no kerberos instance map** *instance*

<b>Syntax Description</b>	<i>instance</i>	Name of a Kerberos instance.
	<i>privilege-level</i>	The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.

## kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** command in global configuration mode. To remove the specified Kerberos realm from this router, use the **no** form of this command.

**kerberos local-realm** *kerberos-realm*

**no kerberos local-realm**

<b>Syntax Description</b>	<i>kerberos-realm</i>	The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters.
---------------------------	-----------------------	---

## kerberos preauth

To specify a preauthentication method to use to communicate with the key distribution center (KDC), use the **kerberos preauth** command in global configuration mode. To disable Kerberos preauthentication, use the **no** form of this command.

```
kerberos preauth [encrypted-unix-timestamp | encrypted-kerberos-timestamp | none]
```

```
no kerberos preauth
```

Syntax Description		
	<b>encrypted-unix-timestamp</b>	(Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.
	<b>encrypted-kerberos-timestamp</b>	(Optional) Use the RFC1510 kerberos timestamp as a quick authentication method when communicating with the KDC.
	<b>none</b>	(Optional) Do not use Kerberos preauthentication.

## kerberos realm

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the **kerberos realm** command in global configuration mode. To remove a Kerberos realm map, use the **no** form of this command.

```
kerberos realm {dns-domain | host} kerberos-realm
```

```
no kerberos realm {dns-domain | host} kerberos-realm
```

Syntax Description		
	<i>dns-domain</i>	Name of a DNS domain or host.
	<i>host</i>	Name of a DNS host.
	<i>kerberos-realm</i>	Name of the Kerberos realm to which the specified domain or host belongs.

## kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server** command in global configuration mode. To remove a Kerberos server for a specified Kerberos realm, use the **no** form of this command.

```
kerberos server kerberos-realm {hostname | ip-address} [port-number]
```

```
no kerberos server kerberos-realm {hostname | ip-address}
```

Syntax Description		
<i>kerberos-realm</i>		Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
<i>hostname</i>		Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).
<i>ip-address</i>		IP address of the host functioning as the Kerberos server for the specified Kerberos realm.
<i>port-number</i>		(Optional) Port that the key distribution center (KDC) monitors (defaults to 88).

## kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab entry** command in global configuration mode. To remove a SRVTAB entry from the router's configuration, use the **no** form of this command.

**kerberos srvtab entry** *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*

**no kerberos srvtab entry** *kerberos-principal principal-type*

Syntax Description		
<i>kerberos-principal</i>		A service on the router.
<i>principal-type</i>		Version of the Kerberos SRVTAB.
<i>timestamp</i>		Number representing the date and time the SRVTAB entry was created.
<i>key-version number</i>		Version of the encryption key format.
<i>key-type</i>		Type of encryption used.
<i>key-length</i>		Length, in bytes, of the encryption key.
<i>encrypted-keytab</i>		Secret key the router shares with the key distribution center (KDC). It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.

## kerberos srvtab remote

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab remote** command in global configuration mode.

**kerberos srvtab remote** {boot\_device:*URL*}

Syntax Description		
<i>URL</i>		Machine that has the Kerberos SRVTAB file.
<i>ip-address</i>		IP address of the machine that has the Kerberos SRVTAB file.
<i>filename</i>		Name of the SRVTAB file.

## key config-key

To define a private DES key for the router, use the **key config-key** command in global configuration mode. To delete a private Data Encryption Standard (DES) key from the router, use the **no** form of this command.

```
key config-key 1 string
```

```
no key config-key 1 string
```

---

**Syntax Description**

---

<b>1</b>	Key number. This number is always 1.
<i>string</i>	Private DES key (can be up to eight alphanumeric characters).

---

## show kerberos creds

To display the contents of your credentials cache, use the **show kerberos creds** command in privileged EXEC mode.

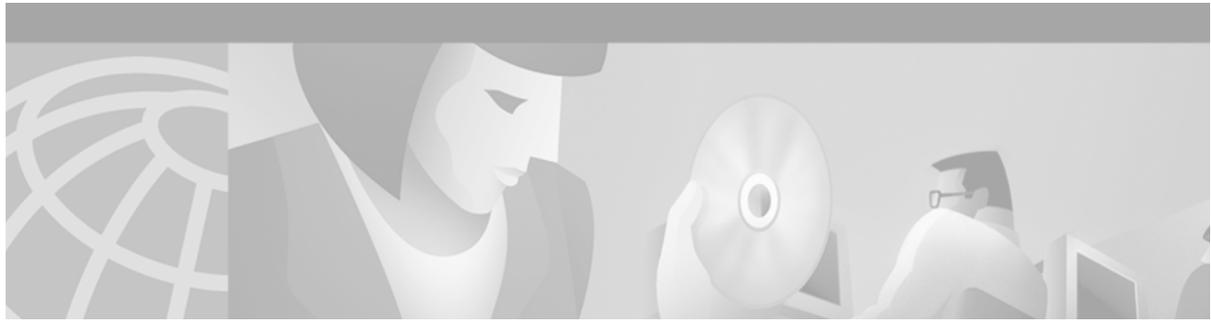
```
show kerberos creds
```

---

**Syntax Description**

This command has no arguments or keywords.

■ show kerberos creds



## Lock-and-Key Commands

---

This chapter describes the function and syntax of the Lock-and-Key commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### access-enable

To enable the router to create a temporary access list entry in a dynamic access list, use the **access-enable EXEC** command.

```
access-enable [host] [timeout minutes]
```

<b>Syntax Description</b>	<b>host</b>	(Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network.
	<b>timeout <i>minutes</i></b>	(Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection.

### access-list dynamic-extend

To allow the absolute timer of the dynamic access control list (ACL) to be extended an additional six minutes, use the **access-list dynamic-extend** command in global configuration mode. To disable this functionality, use the **no** form of this command.

```
access-list dynamic-extend
```

```
no access-list dynamic-extend
```

**Syntax Description** This command has no arguments or keywords.

## access-template

To manually place a temporary access list entry on a router to which you are connected, use the **access-template EXEC** command.

```
access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout
minutes]
```

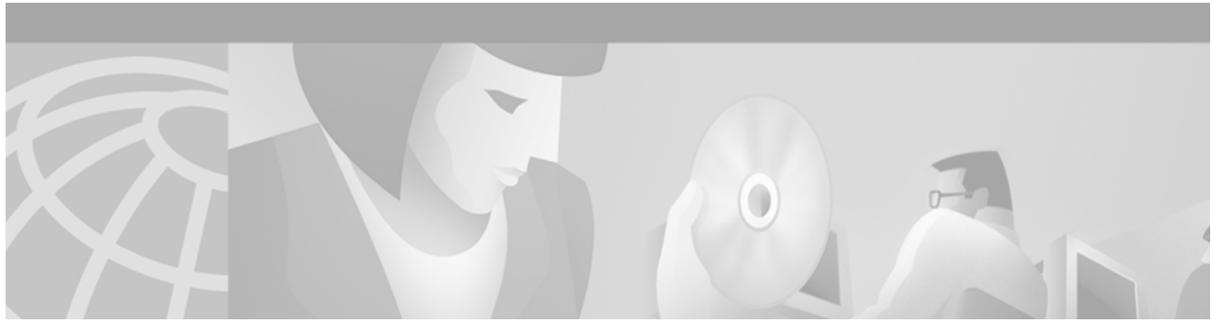
Syntax Description	
<i>access-list-number</i>	(Optional) Number of the dynamic access list.
<i>name</i>	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
<i>dynamic-name</i>	(Optional) Name of a dynamic access list.
<i>source</i>	(Optional) Source address in a dynamic access list. The keywords <i>host</i> and <i>any</i> are allowed. All other attributes are inherited from the original access-list entry.
<i>destination</i>	(Optional) Destination address in a dynamic access list. The keywords <i>host</i> and <i>any</i> are allowed. All other attributes are inherited from the original access-list entry.
<b>timeout</b> <i>minutes</i>	(Optional) Specifies a maximum time limit for each entry within this dynamic list. This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently.

## clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template EXEC** command.

```
clear access-template [access-list-number | name] [dynamic-name] [source] [destination]
```

Syntax Description	
<i>access-list-number</i>	(Optional) Number of the dynamic access list from which the entry is to be deleted.
<i>name</i>	(Optional) Name of an IP access list from which the entry is to be deleted. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
<i>dynamic-name</i>	(Optional) Name of the dynamic access list from which the entry is to be deleted.
<i>source</i>	(Optional) Source address in a temporary access list entry to be deleted.
<i>destination</i>	(Optional) Destination address in a temporary access list entry to be deleted.



## Reflexive Access List Commands

---

This chapter describes the function and syntax of the reflexive access list commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### evaluate

To nest a reflexive access list within an access list, use the **evaluate** command in access-list configuration mode. To remove a nested reflexive access list from the access list, use the **no** form of this command.

**evaluate** *name*

**no evaluate** *name*

---

<b>Syntax Description</b>	<i>name</i>	The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the <b>permit</b> (reflexive) command.
---------------------------	-------------	---

---

### ip reflexive-list timeout

To specify the length of time that reflexive access list entries will continue to exist when no packets in the session are detected, use the **ip reflexive-list timeout** command in global configuration mode. To reset the timeout period to the default timeout, use the **no** form of this command.

**ip reflexive-list timeout** *seconds*

**no ip reflexive-list timeout**

---

<b>Syntax Description</b>	<i>seconds</i>	Specifies the number of seconds to wait (when no session traffic is being detected) before temporary access list entries expire. Use a positive integer from 0 to $2^{32}-1$ . The default is 300 seconds.
---------------------------	----------------	--

---

## permit (reflexive)

To create a reflexive access list and to enable its temporary entries to be automatically generated, use the **permit** command in access-list configuration mode. To delete the reflexive access list (if only one protocol was defined) or to delete protocol entries from the reflexive access list (if multiple protocols are defined), use the **no** form of this command.

**permit** *protocol source source-wildcard destination destination-wildcard reflect name [timeout seconds]*

**no permit** *protocol source-wildcard destination destination-wildcard reflect name*

### Syntax Description

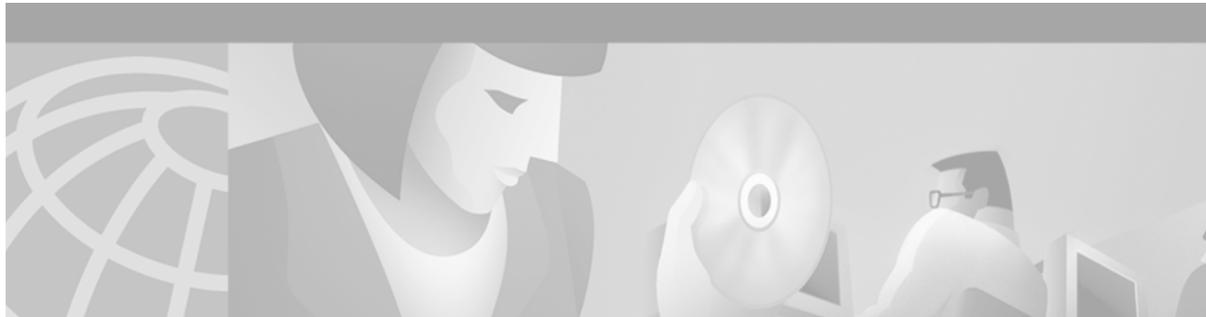
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords <b>gre</b> , <b>icmp</b> , <b>ip</b> , <b>ipinip</b> , <b>nos</b> , <b>tcp</b> , or <b>udp</b> , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol, Transmission Control Protocol, and User Datagram Protocol), use the keyword <b>ip</b> .
<i>source</i>	Number of the network or host from which the packet is being sent. There are three other ways to specify the source: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format.</li> <li>• Use the keyword <b>any</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally not recommended.</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.</li> </ul>
<i>source-wildcard</i>	Wildcard bits (mask) to be applied to source. There are three other ways to specify the source wildcard: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</li> <li>• Use the keyword <b>any</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally not recommended.</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.</li> </ul>
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three other ways to specify the destination: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format.</li> <li>• Use the keyword <b>any</b> as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally not recommended.</li> <li>• Use <b>host destination</b> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.</li> </ul>

---

<i>destination-wildcard</i>	Wildcard bits to be applied to the destination. There are three other ways to specify the destination wildcard: <ul style="list-style-type: none"><li>• Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</li><li>• Use the keyword <b>any</b> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. This keyword is normally <i>not</i> recommended.</li><li>• Use <b>host</b> <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.</li></ul>
<b>reflect</b>	Identifies this access list as a reflexive access list.
<i>name</i>	Specifies the name of the reflexive access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists. The name can be up to 64 characters long.
<b>timeout</b> <i>seconds</i>	(Optional) Specifies the number of seconds to wait (when no session traffic is being detected) before entries expire in this reflexive access list. Use a positive integer from 0 to $2^{32}-1$ . If not specified, the number of seconds defaults to the global timeout value.

---

■ permit (reflexive)



## TCP Intercept Commands

---

This chapter describes the function and syntax of the TCP intercept commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### ip tcp intercept connection-timeout

To change how long a TCP connection will be managed by the TCP intercept after no activity, use the **ip tcp intercept connection-timeout** global configuration command. To restore the default, use the **no** form of this command.

**ip tcp intercept connection-timeout** *seconds*

**no ip tcp intercept connection-timeout** [*seconds*]

<b>Syntax Description</b>	<i>seconds</i>	Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24 hours).
---------------------------	----------------	--

### ip tcp intercept drop-mode

To set the TCP intercept drop mode, use the **ip tcp intercept drop-mode** global configuration command. To restore the default, use the **no** form of this command.

**ip tcp intercept drop-mode** [*oldest* | *random*]

**no ip tcp intercept drop-mode** [*oldest* | *random*]

<b>Syntax Description</b>	<i>oldest</i>	(Optional) Software drops the oldest partial connection. This is the default.
	<i>random</i>	(Optional) Software drops a randomly selected partial connection.

## ip tcp intercept finrst-timeout

To change how long after receipt of a reset or FIN-exchange the software ceases to manage the connection, use the **ip tcp intercept finrst-timeout** global configuration command. To restore the default, use the **no** form of this command.

**ip tcp intercept finrst-timeout** *seconds*

**no ip tcp intercept finrst-timeout** [*seconds*]

<b>Syntax Description</b>	<i>seconds</i>	Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds.
---------------------------	----------------	---

## ip tcp intercept list

To enable TCP intercept, use the **ip tcp intercept list** global configuration command. To disable TCP intercept, use the **no** form of this command.

**ip tcp intercept list** *access-list-number*

**no ip tcp intercept list** *access-list-number*

<b>Syntax Description</b>	<i>access-list-number</i>	Extended access list number in the range from 100 to 199.
---------------------------	---------------------------	---

## ip tcp intercept max-incomplete high

To define the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete high** global configuration command. To restore the default, use the **no** form of this command.

**ip tcp intercept max-incomplete high** *number*

**no ip tcp intercept max-incomplete high** [*number*]

<b>Syntax Description</b>	<i>number</i>	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.
---------------------------	---------------	--

## ip tcp intercept max-incomplete low

To define the number of incomplete connections below which the software leaves aggressive mode, use the **ip tcp intercept max-incomplete low** global configuration command. To restore the default, use the **no** form of this command.

```
ip tcp intercept max-incomplete low number
```

```
no ip tcp intercept max-incomplete low [number]
```

### Syntax Description

<i>number</i>	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900.
---------------	---

## ip tcp intercept mode

To change the TCP intercept mode, use the **ip tcp intercept mode** global configuration command. To restore the default, use the **no** form of this command.

```
ip tcp intercept mode {intercept | watch}
```

```
no ip tcp intercept mode [intercept | watch]
```

### Syntax Description

<b>intercept</b>	Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.
<b>watch</b>	Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.

## ip tcp intercept one-minute high

To define the number of connection requests received in the last one-minute sample period before the software enters aggressive mode, use the **ip tcp intercept one-minute high** global configuration command. To restore the default, use the **no** form of this command.

```
ip tcp intercept one-minute high number
```

```
no ip tcp intercept one-minute high [number]
```

### Syntax Description

<i>number</i>	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.
---------------	--

## ip tcp intercept one-minute low

To define the number of connection requests below which the software leaves aggressive mode, use the **ip tcp intercept one-minute low** global configuration command. To restore the default, use the **no** form of this command.

**ip tcp intercept one-minute low** *number*

**no ip tcp intercept one-minute low** [*number*]

---

### Syntax Description

<i>number</i>	Defines the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.
---------------	--

---

## ip tcp intercept watch-timeout

To define how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server, use the **ip tcp intercept watch-timeout** global configuration command. To restore the default, use the **no** form of this command.

**ip tcp intercept watch-timeout** *seconds*

**no ip tcp intercept watch-timeout** [*seconds*]

---

### Syntax Description

<i>seconds</i>	Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.
----------------	---

---

## show tcp intercept connections

To display TCP incomplete and established connections, use the **show tcp intercept connections** EXEC command.

**show tcp intercept connections**

---

### Syntax Description

This command has no arguments or keywords.

## show tcp intercept statistics

To display TCP intercept statistics, use the **show tcp intercept statistics** EXEC command.

**show tcp intercept statistics**

---

### Syntax Description

This command has no arguments or keywords.



## Context-Based Access Control Commands

---

This chapter describes the function and syntax of the Context-based Access Control (CBAC) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### ip inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the **ip inspect alert off** command in global configuration mode. To enable CBAC alert messages, use the **no** form of this command.

**ip inspect alert-off**

**no ip inspect alert-off**

---

**Syntax Description** This command has no arguments or keywords.

### ip inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each CBAC session closes, use the **ip inspect audit trail** command in global configuration mode. To turn off CBAC audit trail message, use the **no** form of this command.

**ip inspect audit trail**

**no ip inspect audit trail**

---

**Syntax Description** This command has no arguments or keywords.

## ip inspect dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity), use the **ip inspect dns-timeout** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

**ip inspect dns-timeout** *seconds*

**no ip inspect dns-timeout**

<b>Syntax Description</b>	<i>seconds</i>	Specifies the length of time in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5 seconds.
---------------------------	----------------	--

## ip inspect

To apply a set of inspection rules to an interface, use the **ip inspect** command in interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

**ip inspect** *inspection-name* {**in** | **out**}

**no ip inspect** *inspection-name* {**in** | **out**}

<b>Syntax Description</b>	<i>inspection-name</i>	Identifies which set of inspection rules to apply.
	<b>in</b>	Applies the inspection rules to inbound traffic.
	<b>out</b>	Applies the inspection rules to outbound traffic.

## ip inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the **ip inspect max-incomplete high** command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

**ip inspect max-incomplete high** *number*

**no ip inspect max-incomplete high**

<b>Syntax Description</b>	<i>number</i>	Specifies the number of existing half-open sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.
---------------------------	---------------	---

## ip inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect max-incomplete low** command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

**ip inspect max-incomplete low** *number*

**no ip inspect max-incomplete low**

### Syntax Description

<i>number</i>	Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.
---------------	--

## ip inspect name

To define a set of inspection rules, use the **ip inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

**ip inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]

**no ip inspect name** [*inspection-name protocol*]

### HTTP Inspection Syntax

**ip inspect name** *inspection-name http* [**java-list** *access-list*] [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*] (Java protocol only)

**no ip inspect name** *inspection-name protocol* (removes the inspection rule for a protocol)

### RPC Inspection Syntax

**ip inspect name** *inspection-name rpc program-number number* [**wait-time** *minutes*] [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*] (RPC protocol only)

**no ip inspect name** *inspection-name protocol* (removes the inspection rule for a protocol)

### Fragment Inspection Syntax

**ip inspect name** *inspection-name fragment* [**max** *number* **timeout** *seconds*]

**no ip inspect name** *inspection-name fragment* (removes fragment inspection for a rule)

### Syntax Description

<i>inspection-name</i>	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same <i>inspection-name</i> as the existing set of rules.
<i>protocol</i>	A protocol keyword listed in Table 28 or Table 29.

<b>alert</b> {on   off}	(Optional) For each inspected protocol, the generation of alert messages can be set be <b>on</b> or <b>off</b> . If no option is selected, alerts are generated based on the setting of the <b>ip inspect alert-off</b> command.
<b>audit-trail</b> {on   off}	(Optional) For each inspected protocol, audit trail can be set <b>on</b> or <b>off</b> . If no option is selected, audit trail message are generated based on the setting of the <b>ip inspect audit-trail</b> command.
<b>http</b>	(Optional) Specifies the HTTP protocol for Java applet blocking.
<b>timeout</b> <i>seconds</i>	(Optional) To override the global TCP or User Datagram Protocol idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout.  This timeout overrides the global TCP and UDP timeouts but will not override the global Domain Name System timeout.
<b>java-list</b> <i>access-list</i>	(Optional) Specifies the access list (name or number) to use to determine “friendly” sites. This keyword is available only for the HTTP protocol, for Java applet blocking. Java blocking only works with standard access lists.
<b>rpc program-number</b> <i>number</i>	Specifies the program number to permit. This keyword is available only for the remote-procedure call protocol.
<b>wait-time</b> <i>minutes</i>	(Optional) Specifies the number of minutes to keep a small hole in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait-time is zero minutes. This keyword is available only for the RPC protocol.
<b>fragment</b>	Specifies fragment inspection for the named rule.
<b>max</b> <i>number</i>	(Optional) Specifies the maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries.  Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.
<b>timeout</b> <i>seconds</i> (fragmentation)	(Optional) Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is one second.  If this number is set to a value greater than one second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

**Table 28 Protocol Keywords—Transport-Layer Protocols**

Protocol	Keyword
TCP	<b>tcp</b>
UDP	<b>udp</b>

**Table 29 Protocol Keywords—Application-Layer Protocols**

Protocol	Keyword
CU-SeeMe	<b>cuseeme</b>
FTP	<b>ftp</b>
Java	<b>http</b>
H.323	<b>h323</b>
Microsoft NetShow	<b>netshow</b>
UNIX R commands (rlogin, rexec, rsh)	<b>rcmd</b>
RealAudio	<b>realaudio</b>
RPC	<b>rpc</b>
SMTP	<b>smtp</b>
SQL*Net	<b>sqlnet</b>
StreamWorks	<b>streamworks</b>
TFTP	<b>tftp</b>
VDOLive	<b>vdolive</b>

## ip inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ip inspect one-minute high** command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

**ip inspect one-minute high** *number*

**no ip inspect one-minute high**

### Syntax Description

<i>number</i>	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.
---------------	--

## ip inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect one-minute low** command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command

**ip inspect one-minute low** *number*

**no ip inspect one-minute low**

### Syntax Description

<i>number</i>	Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.
---------------	---

## ip inspect tcp finwait-time

To define how long a TCP session will still be managed after the firewall detects a FIN-exchange, use the **ip inspect tcp finwait-time** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

**ip inspect tcp finwait-time** *seconds*

**no ip inspect tcp finwait-time**

<b>Syntax Description</b>	<i>seconds</i>	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds.
---------------------------	----------------	---

## ip inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the **ip inspect tcp idle-time** command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the **no** form of this command.

**ip inspect tcp idle-time** *seconds*

**no ip inspect tcp idle-time**

<b>Syntax Description</b>	<i>seconds</i>	Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).
---------------------------	----------------	---

## ip inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service detection and prevention, use the **ip inspect tcp max-incomplete host** command in global configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

**ip inspect tcp max-incomplete host** *number* **block-time** *minutes*

**no ip inspect tcp max-incomplete host**

<b>Syntax Description</b>	<i>number</i>	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions.
	<b>block-time</b>	Specifies blocking of connection initiation to a host.
	<i>minutes</i>	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.

## ip inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ip inspect tcp synwait-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

**ip inspect tcp synwait-time** *seconds*

**no ip inspect tcp synwait-time**

---

**Syntax Description**

*seconds* Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session. The default is 30 seconds.

---

## ip inspect udp idle-time

To specify the User Datagram Protocol idle timeout (the length of time for which a UDP “session” will still be managed while there is no activity), use the **ip inspect udp idle-time** command in global configuration model. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

**ip inspect udp idle-time** *seconds*

**no ip inspect udp idle-time**

---

**Syntax Description**

*seconds* Specifies the length of time a UDP “session” will still be managed while there is no activity. The default is 30 seconds.

---

## no ip inspect

To turn off Context-based Access Control (CBAC) completely at a firewall, use the **no ip inspect** command in global configuration mode.

**no ip inspect**

---

**Syntax Description**

This command has no arguments or keywords.

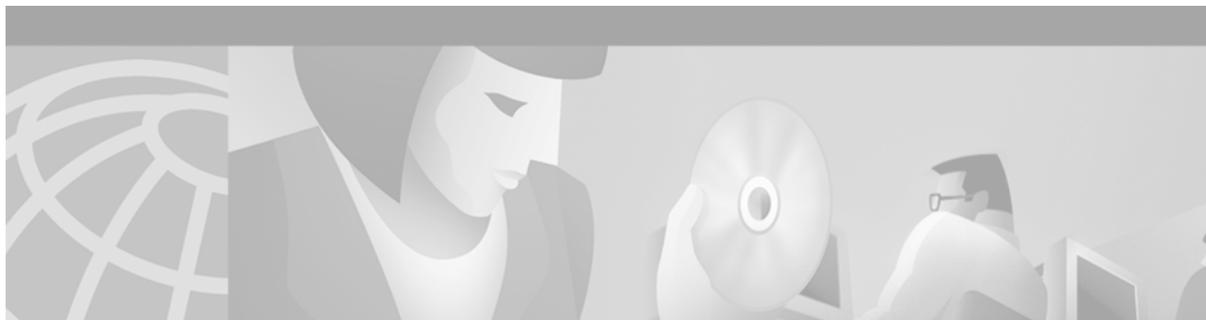
# show ip inspect

To view Context-based Access Control (CBAC) configuration and session information, use the **show ip inspect** command in privileged EXEC mode.

```
show ip inspect { name inspection-name | config | interfaces | session [detail] | all }
```

## Syntax Description

<b>name</b> <i>inspection-name</i>	Displays the configured inspection rule with the name <i>inspection-name</i> .
<b>config</b>	Displays the complete CBAC inspection configuration.
<b>interfaces</b>	Displays interface configuration with respect to applied inspection rules and access lists.
<b>session [detail]</b>	Displays existing sessions that are currently being tracked and inspected by CBAC. The optional <b>detail</b> keyword causes additional details about these sessions to be shown.
<b>all</b>	Displays all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.



# Cisco IOS Firewall Intrusion Detection System Commands

---

This chapter describes the function and syntax of the Cisco IOS Firewall Intrusion Detection System (IDS) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

## clear ip audit configuration

To disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip audit configuration** EXEC command.

**clear ip audit configuration**

**Syntax Description** This command has no arguments or keywords.

## clear ip audit statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip audit statistics** EXEC command.

**clear ip audit statistics**

**Syntax Description** This command has no arguments or keywords.

## ip audit

To apply an audit specification created with the **ip audit** command to a specific interface and for a specific direction, use the **ip audit** interface configuration command. To disable auditing of the interface for the specified direction, use the **no** version of this command.

```
ip audit audit-name {in | out}
```

```
no ip audit audit-name {in | out}
```

### Syntax Description

<i>audit-name</i>	Name of an audit specification.
<b>in</b>	Inbound traffic.
<b>out</b>	Outbound traffic.

## ip audit attack

To specify the default actions for attack signatures, use the **ip audit attack** global configuration command. To set the default action for attack signatures, use the **no** form of this command.

```
ip audit attack {action [alarm] [drop] [reset]}
```

```
no ip audit attack
```

### Syntax Description

<b>action</b>	Specifies an action for the attack signature to take in response to a match.
<b>alarm</b>	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the <b>action</b> keyword.
<b>drop</b>	(Optional) Drops the packet. Used with the <b>action</b> keyword.
<b>reset</b>	(Optional) Resets the TCP session. Used with the <b>action</b> keyword.

## ip audit info

To specify the default actions for info signatures, use the **ip audit info** global configuration command. To set the default action for info signatures, use the **no** form of this command.

```
ip audit info {action [alarm] [drop] [reset]}
```

```
no ip audit info
```

### Syntax Description

<b>action</b>	Sets an action for the info signature to take in response to a match.
<b>alarm</b>	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the <b>action</b> keyword.

<b>drop</b>	(Optional) Drops the packet. Used with the <b>action</b> keyword.
<b>reset</b>	(Optional) Resets the TCP session. Used with the <b>action</b> keyword.

## ip audit name

To create audit rules for info and attack signature types, use the **ip audit name** global configuration command. To delete an audit rule, use the **no** form of this command.

```
ip audit name audit-name {info | attack} [list standard-acl] [action [alarm] [drop] [reset]]
```

```
no ip audit name audit-name {info | attack}
```

Syntax Description		
	<i>audit-name</i>	Name for an audit specification.
	<b>info</b>	Specifies that the audit rule is for info signatures.
	<b>attack</b>	Specifies that the audit rule is for attack signatures.
	<b>list</b>	(Optional) Specifies an ACL to attach to the audit rule.
	<i>standard-acl</i>	(Optional) Integer representing an access control list. Use with the <b>list</b> keyword.
	<b>action</b>	(Optional) Specifies an action or actions to take in response to a match.
	<b>alarm</b>	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Use with the <b>action</b> keyword.
	<b>drop</b>	(Optional) Drops the packet. Use with the <b>action</b> keyword.
	<b>reset</b>	(Optional) Resets the TCP session. Use with the <b>action</b> keyword.

## ip audit notify

To specify the method of event notification, use the **ip audit notify** global configuration command. To disable event notifications, use the **no** form of this command.

```
ip audit notify {nr-director | log}
```

```
no ip audit notify {nr-director | log}
```

Syntax Description		
	<b>nr-director</b>	Send messages in NetRanger format to the NetRanger Director or Sensor.
	<b>log</b>	Send messages in syslog format.

## ip audit po local

To specify the local Post Office parameters used when sending event notifications to the NetRanger Director, use the **ip audit po local** global configuration command. To set the local Post Office parameters to their default settings, use the **no** form of this command.

**ip audit po local** *hostid id-number orgid id-number*

**no ip audit po local** [*hostid id-number orgid id-number*]

Syntax Description	hostid	Specifies a NetRanger host ID.
	<i>id-number (hostid)</i>	Unique integer in the range 1-65535 used in NetRanger communications to identify the local host. Use with the <b>hostid</b> keyword.
	<b>orgid</b>	Specifies a NetRanger organization ID.
	<i>id-number (orgid)</i>	Unique integer in the range 1-65535 used in NetRanger communications to identify the group to which the local host belongs. Use with the <b>orgid</b> keyword.

## ip audit po max-events

To specify the maximum number of event notifications that are placed in the router's event cue, use the **ip audit po max-events** global configuration command. To set the number of recipients to the default setting, use the **no** version of this command.

**ip audit po max-events** *number-of-events*

**no ip audit po max-events**

Syntax Description	<i>number-of-events</i>	Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event cue. The default is 100 events.

## ip audit po protected

To specify whether an address is on a protected network, use the **ip audit po protected** global configuration command. To remove network addresses from the protected network list, use the **no** form of this command. If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

**ip audit po protected** *ip-addr [to ip-addr]*

**no ip audit po protected** [*ip-addr*]

## Syntax Description

<b>to</b>	(Optional) Specifies a range of IP addresses.
<i>ip-addr</i>	IP address of a network host.

## ip audit po remote

To specify one or more set of Post Office parameters for NetRanger Directors receiving event notifications from the router, use the **ip audit po remote** global configuration command. To remove a NetRanger Director's Post Office parameters as defined by host ID, organization ID, and IP address, use the **no** form of this command.

```
ip audit po remote hostid host-id orgid org-id rmtaddress ip-address localaddress ip-address
[port port-number] [preference preference-number] [timeout seconds] [application
{director | logger}]
```

```
no ip audit po remote hostid host-id orgid org-id rmtaddress ip-address
```

## Syntax Description

<i>host-id</i>	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the local host. Use with the <b>hostid</b> keyword.
<b>hostid</b>	Specifies a NetRanger host ID.
<i>org-id</i>	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the group in which the local host belongs. Use with the <b>orgid</b> keyword.
<b>orgid</b>	Specifies a NetRanger organization ID.
<b>rmtaddress</b>	Specifies the IP address of the NetRanger Director.
<b>localaddress</b>	Specifies the IP address of the Cisco IOS Firewall IDS router.
<i>ip-address</i>	IP address of the NetRanger Director or Cisco IOS Firewall IDS router's interface. Use with the <b>rmtaddress</b> and <b>localaddress</b> keywords.
<i>port-number</i>	(Optional) Integer representing the UDP port on which the NetRanger Director is listening for event notifications. Use with the <b>port</b> keyword.
<b>port</b>	(Optional) Specifies a User Datagram Protocol port through which to send messages.
<b>preference</b>	(Optional) Specifies a route preference for communication.
<i>preference-number</i>	(Optional) Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. Use with the <b>preference</b> keyword.
<i>seconds</i>	(Optional) Integer representing the heartbeat timeout value for Post Office communications. Use with the <b>timeout</b> keyword.
<b>timeout</b>	(Optional) Specifies a timeout value for Post Office communications.
<b>application</b>	(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IDS messages.
<b>director</b>	(Optional) Specifies that the receiving application is the NetRanger Director interface.
<b>logger</b>	(Optional) Specifies that the receiving application is a NetRanger Sensor.

## ip audit signature

To attach a policy to a signature, use the **ip audit signature** global configuration command. You can set two policies: disable a signature or qualify the audit of a signature with an access list. To remove the policy, use the **no** form of this command. If the policy disabled a signature, then the **no** form of this command reenables the signature. If the policy attached an access list to the signature, the **no** form of this command removes the access list.

```
ip audit signature signature-id {disable | list acl-list}
```

```
no ip audit signature signature-id
```

<b>Syntax Description</b>	<i>signature-id</i>	Unique integer specifying a signature as defined in the NetRanger Network Security Database.
	<b>disable</b>	Disables the ACL associated with the signature.
	<b>list</b>	Specifies an ACL to associate with the signature.
	<i>acl-list</i>	Unique integer specifying a configured ACL on the router. Use with the <b>list</b> keyword.

## ip audit smtp

To specify the number of recipients in a mail message over which a spam attack is suspected, use the **ip audit smtp** global configuration command. To set the number of recipients to the default setting, use the **no** form of this command.

```
ip audit smtp spam number-of-recipients
```

```
no ip audit smtp spam
```

<b>Syntax Description</b>	<b>spam</b>	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
	<i>number-of-recipients</i>	Integer in the range of 1 to 65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the <b>spam</b> keyword. The default is 250 recipients.

## show ip audit configuration

To display additional configuration information, including default values that may not be displayed using the **show run** command, use the **show ip audit configuration EXEC** command.

```
show ip audit configuration
```

<b>Syntax Description</b>	This command has no argument or keywords.
---------------------------	---

## show ip audit interface

To display the interface configuration, use the **show ip audit interface** EXEC command.

```
show ip audit interface
```

---

**Syntax Description** This command has no arguments or keywords.

## show ip audit statistics

To display the number of packets audited and the number of alarms sent, among other information, use the **show ip audit statistics** EXEC command.

```
show ip audit statistics
```

---

**Syntax Description** This command has no arguments or keywords.

■ show ip audit statistics



## Authentication Proxy Commands

---

This chapter describes the function and syntax of the authentication proxy commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

```
clear ip auth-proxy cache [* | host-ip-address]
```

---

**Syntax Description**

*	Clears all authentication proxy entries, including user profiles and dynamic access lists.
<i>host-ip-address</i>	Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host.

---

### ip auth-proxy

To apply an authentication proxy rule at a firewall interface, use the **ip auth-proxy** command in interface configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

```
ip auth-proxy auth-proxy-name
```

```
no ip auth-proxy auth-proxy-name
```

---

**Syntax Description**

<i>auth-proxy-name</i>	Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the <b>ip auth-proxy name</b> command.
------------------------	---

---

## ip auth-proxy auth-cache-time

To set the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity), use the **ip auth-proxy auth-cache-time** command in global configuration mode. To set the default value, use the **no** form of this command.

**ip auth-proxy auth-cache-time** *min*

**no ip auth-proxy auth-cache-time**

<b>Syntax Description</b>	<i>min</i>	Specifies the length of time in minutes that an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes.
---------------------------	------------	--

## ip auth-proxy auth-proxy-banner

To display the router name in the authentication proxy login page, use the **ip auth-proxy auth-proxy-banner** command in global configuration mode. To disable display of the router name, use the **no** form of this command.

**ip auth-proxy auth-proxy-banner**

**no ip auth-proxy auth-proxy-banner**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## ip auth-proxy name

To create an authentication proxy rule, use the **ip auth-proxy name** command in global configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

**ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** *std-access-list*]

**no ip auth-proxy name** *auth-proxy-name*

<b>Syntax Description</b>	<i>auth-proxy-name</i>	Associates a name with an authentication proxy rule. Enter a name of up to 16 alphanumeric characters.
	<b>http</b>	Specifies the protocol that triggers the authentication proxy. The only supported protocol is HTTP.

---

<b>auth-cache-time</b> <i>min</i>	(Optional) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 2,147,483,647. The default value is equal to the value set with the <b>ip auth-proxy auth-cache-time</b> command.
<b>list</b> <i>std-access-list</i>	(Optional) Specifies a standard access list to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the standard access list. If no list is specified, all connections initiating HTTP traffic arriving at the interface are subject to authentication.

---

## show ip auth-proxy

To display the authentication proxy entries or the running authentication proxy configuration, use the **show ip auth-proxy** command in privileged EXEC mode.

```
show ip auth-proxy {cache | configuration}
```

---

### Syntax Description

---

<b>cache</b>	Display the current list of the authentication proxy entries.
<b>configuration</b>	Display the running authentication proxy configuration.

---

■ show ip auth-proxy



## Port to Application Mapping Commands

---

This chapter describes the function and syntax of the Port to Application Mapping (PAM) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### ip port-map

To establish Port to Application Mapping (PAM), use the **ip port-map** global configuration command. To delete user-defined PAM entries, use the **no** form of this command.

```
ip port-map appl_name port port_num [list acl_num]
```

```
no ip port-map appl_name port port_num [list acl_num]
```

---

#### Syntax Description

<i>appl_name</i>	Specifies the name of the application with which to apply the port mapping.
<b>port</b>	Indicates that a port number maps to the application.
<i>port_num</i>	Identifies a port number in the range 1 to 65535.
<b>list</b>	(Optional) Indicates that the port mapping information applies to a specific host or subnet.
<i>acl_num</i>	(Optional) Identifies the standard access control list (ACL) number used with PAM.

---

# show ip port-map

To display the Port to Application Mapping (PAM) information, use the **show ip port-map** privileged EXEC command.

```
show ip port-map [appl_name | port port_num]
```

---

**Syntax Description**

---

<i>appl_name</i>	(Optional) Specifies the name of the application to which to apply the port mapping.
<b>port</b> <i>port_num</i>	(Optional) Specifies the alternative port number that maps to the application.

---



## IPSec Network Security Commands

---

This chapter describes the function and syntax of the IPSec network security commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### clear crypto sa

To delete IP Security security associations, use the **clear crypto sa** EXEC command.

**clear crypto sa**

**clear crypto sa peer** {*ip-address* | *peer-name*}

**clear crypto sa map** *map-name*

**clear crypto sa entry** *destination-address protocol spi*

**clear crypto sa counters**

---

#### Syntax Description

<b>peer</b>	Deletes any IPSec security associations for the specified peer.
<i>ip-address</i>	Specifies a remote peer's IP address.
<i>peer-name</i>	Specifies a remote peer's name as the fully qualified domain name, for example remotepeer.example.com.
<b>map</b>	Deletes any IPSec security associations for the named crypto map set.
<i>map-name</i>	Specifies the name of a crypto map set.
<b>entry</b>	Deletes the IPSec security association with the specified address, protocol, and SPI.
<i>destination-address</i>	Specifies the IP address of your peer or the remote peer.
<i>protocol</i>	Specifies either the Encapsulation Security Protocol or Authentication Header.
<i>spi</i>	Specifies an SPI (found by displaying the security association database).
<b>counters</b>	Clears the traffic counters maintained for each security association; <b>counters</b> does not clear the security associations themselves.

## crypto dynamic-map

To create a dynamic crypto map entry and enter the crypto map configuration command mode, use the **crypto dynamic-map** global configuration command. To delete a dynamic crypto map set or entry, use the **no** form of this command.

**crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num*

**no crypto dynamic-map** *dynamic-map-name* [*dynamic-seq-num*]

### Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the number of the dynamic crypto map entry.

## crypto ipsec security-association lifetime

To change global lifetime values used when negotiating IPSec security associations, use the **crypto ipsec security-association lifetime** global configuration command. To reset a lifetime to the default value, use the **no** form of this command.

**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

**no crypto ipsec security-association lifetime** {**seconds** | **kilobytes**}

### Syntax Description

<b>seconds</b> <i>seconds</i>	Specifies the number of seconds a security association will live before expiring. The default is 3600 seconds (one hour).
<b>kilobytes</b> <i>kilobytes</i>	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.

## crypto ipsec transform-set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** global configuration command. To delete a transform set, use the **no** form of the command.

**crypto ipsec transform-set** *transform-set-name* *transform1* [*transform2* [*transform3*]]

**no crypto ipsec transform-set** *transform-set-name*

### Syntax Description

<i>transform-set-name</i>	Specifies the name of the transform set to create (or modify).
<i>transform1</i>	Specifies up to three “transforms.” These transforms define the IPSec security protocols and algorithms.
<i>transform2</i>	
<i>transform3</i>	

## crypto map (global IPSec)

To create or modify a crypto map entry and enter the crypto map configuration mode, use the **crypto map** global configuration command. To delete a crypto map entry or set, use the **no** form of this command.

```
crypto map map-name seq-num ipsec-manual
```

```
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name] [discover]
```

```
no crypto map map-name [seq-num]
```



### Note

Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

### Syntax Description

<i>transform-set-name</i>	Specifies the name of the transform set to create (or modify).
<i>transform1</i>	Specifies up to three “transforms.” These transforms define the IPSec security protocols and algorithms.
<i>transform2</i>	
<i>transform3</i>	

## crypto map (interface IPSec)

To apply a previously defined crypto map set to an interface, use the **crypto map** interface configuration command. To remove the crypto map set from the interface, use the **no** form of this command.

```
crypto map map-name
```

```
no crypto map [map-name]
```

### Syntax Description

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.  When the <b>no</b> form of the command is used, this argument is optional. Any value supplied for the argument is ignored.
-----------------	---

## crypto map local-address

To specify and name an identifying interface to be used by the crypto map for IPSec traffic, use the **crypto map local-address** global configuration command. To remove this command from the configuration, use the **no** form of this command.

```
crypto map map-name local-address interface-id
```

```
no crypto map map-name local-address
```

<b>Syntax Description</b>	<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
	<i>interface-id</i>	The identifying interface that should be used by the router to identify itself to remote peers.  If Internet Key Exchange is enabled and you are using a certification authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates.

## match address (IPSec)

To specify an extended access list for a crypto map entry, use the **match address** crypto map configuration command. To remove the extended access list from a crypto map entry, use the **no** form of this command.

**match address** [*access-list-id* | *name*]

**no match address** [*access-list-id* | *name*]

<b>Syntax Description</b>	<i>access-list-id</i>	(Optional) Identifies the extended access list by its name or number. This value should match the <i>access-list-number</i> or <i>name</i> argument of the extended access list being matched.
	<i>name</i>	(Optional) Identifies the named encryption access list. This name should match the <i>name</i> argument of the named encryption access list being matched.

## mode (IPSec)

To change the mode for a transform set, use the **mode** crypto transform configuration command. To reset the mode to the default value of tunnel mode, use the **no** form of the command.

**mode** [**tunnel** | **transport**]

**no mode**

<b>Syntax Description</b>	<b>tunnel</b>   <b>transport</b>	(Optional) Specifies the mode for a transform set: either tunnel or transport mode. If neither <b>tunnel</b> nor <b>transport</b> is specified, the default (tunnel mode) is assigned.
---------------------------	----------------------------------	--

## set peer (IPSec)

To specify an IP Security peer in a crypto map entry, use the **set peer** crypto map configuration command. To remove an IPSec peer from a crypto map entry, use the **no** form of this command.

```
set peer {hostname | ip-address}
```

```
no set peer {hostname | ip-address}
```

Syntax Description	
<i>hostname</i>	Specifies the IPSec peer by its host name. This is the peer's host name concatenated with its domain name (for example, myhost.example.com).
<i>ip-address</i>	Specifies the IPSec peer by its IP address.

## set pfs

To specify that IP Security should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations, use the **set pfs** crypto map configuration command. To specify that IPSec should not request PFS, use the **no** form of the command.

```
set pfs [group1 | group2]
```

```
no set pfs
```

Syntax Description	
<i>group1</i>	(Optional) Specifies that IPSec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
<i>group2</i>	(Optional) Specifies that IPSec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

## set security-association level per-host

To specify that separate IP Security security associations should be requested for each source/destination host pair, use the **set security-association level per-host** crypto map configuration command. To specify that one security association should be requested for each crypto map access list **permit** entry, use the **no** form of this command.

```
set security-association level per-host
```

```
no set security-association level per-host
```

Syntax Description	
	This command has no arguments or keywords.

## set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security security associations, use the **set security-association lifetime** crypto map configuration command. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

```
set security-association lifetime {seconds seconds | kilobytes kilobytes}
```

```
no set security-association lifetime {seconds | kilobytes}
```

### Syntax Description

<b>seconds</b> <i>seconds</i>	Specifies the number of seconds a security association will live before expiring.
<b>kilobytes</b> <i>kilobytes</i>	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires.

## set session-key

To manually specify the IP Security session keys within a crypto map entry, use the **set session-key** crypto map configuration command. This command is only available for **ipsec-manual** crypto map entries. To remove IPSec session keys from a crypto map entry, use the **no** form of this command.

```
set session-key {inbound | outbound} ah spi hex-key-string
```

```
set session-key {inbound | outbound} esp spi cipher hex-key-string [authenticator  
hex-key-string]
```

```
no set session-key {inbound | outbound} ah
```

```
no set session-key {inbound | outbound} esp
```

### Syntax Description

<b>inbound</b>	Sets the inbound IPSec session key. (You must set both inbound and outbound keys.)
<b>outbound</b>	Sets the outbound IPSec session key. (You must set both inbound and outbound keys.)
<b>ah</b>	Sets the IPSec session key for the Authentication Header protocol. Use when the crypto map entry's transform set includes an AH transform.
<b>esp</b>	Sets the IPSec session key for the Encapsulation Security Protocol. Use when the crypto map entry's transform set includes an ESP transform.
<i>spi</i>	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4,294,967,295 (FFFF FFFF).  You can assign the same SPI to both directions and both protocols. However, not all peers have the same flexibility in SPI assignment. For a given destination address/protocol combination, unique SPI values must be used. The destination address is that of the router if inbound, the peer if outbound.

<i>hex-key-string</i>	<p>Specifies the session key; enter in hexadecimal format.</p> <p>This is an arbitrary hexadecimal string of 8, 16, or 20 bytes.</p> <p>If the crypto map's transform set includes a DES algorithm, specify at least 8 bytes per key.</p> <p>If the crypto map's transform set includes an MD5 algorithm, specify at least 16 bytes per key.</p> <p>If the crypto map's transform set includes an SHA algorithm, specify 20 bytes per key.</p> <p>Keys longer than the above sizes are simply truncated.</p>
<i>cipher</i>	Indicates that the key string is to be used with the ESP encryption transform.
<b>authenticator</b>	(Optional) Indicates that the key string is to be used with the ESP authentication transform. This argument is required only when the crypto map entry's transform set includes an ESP authentication transform.

## set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set** crypto map configuration command. To remove all transform sets from a crypto map entry, use the **no** form of this command.

**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]

**no set transform-set**

### Syntax Description

<i>transform-set-name</i>	<p>Name of the transform set.</p> <p>For an <b>ipsec-manual</b> crypto map entry, you can specify only one transform set.</p> <p>For an <b>ipsec-isakmp</b> or dynamic crypto map entry, you can specify up to 6 transform sets.</p>
---------------------------	--

## show crypto dynamic-map

To view a dynamic crypto map set, use the **show crypto dynamic-map EXEC** command.

**show crypto dynamic-map** [**tag** *map-name*]

### Syntax Description

<b>tag</b> <i>map-name</i>	(Optional) Displays only the crypto dynamic map set with the specified <i>map-name</i> .
----------------------------	--

## show crypto ipsec sa

To view the settings used by current security associations, use the **show crypto ipsec sa** EXEC command.

```
show crypto ipsec sa [map map-name | address | identity] [detail]
```

Syntax Description		
<b>map</b> <i>map-name</i>	(Optional) Displays any existing security associations created for the crypto map set named <i>map-name</i> .	
<b>address</b>	(Optional) Displays the all existing security associations, sorted by the destination address (either the local address or the address of the IP Security remote peer) and then by protocol (Authentication Header or Encapsulation Security Protocol).	
<b>identity</b>	(Optional) Displays only the flow information. It does not show the security association information.	
<b>detail</b>	(Optional) Displays detailed error counters. (The default is the high level send/receive error counters.)	

## show crypto ipsec security-association lifetime

To view the security-association lifetime value configured for a particular crypto map entry, use the **show crypto ipsec security-association lifetime** EXEC command.

```
show crypto ipsec security-association lifetime
```

Syntax Description	
	This command has no arguments or keywords.

## show crypto ipsec transform-set

To view the configured transform sets, use the **show crypto ipsec transform-set** EXEC command.

```
show crypto ipsec transform-set [tag transform-set-name]
```

Syntax Description	
<b>tag</b> <i>transform-set-name</i>	(Optional) Displays only the transform sets with the specified <i>transform-set-name</i> .

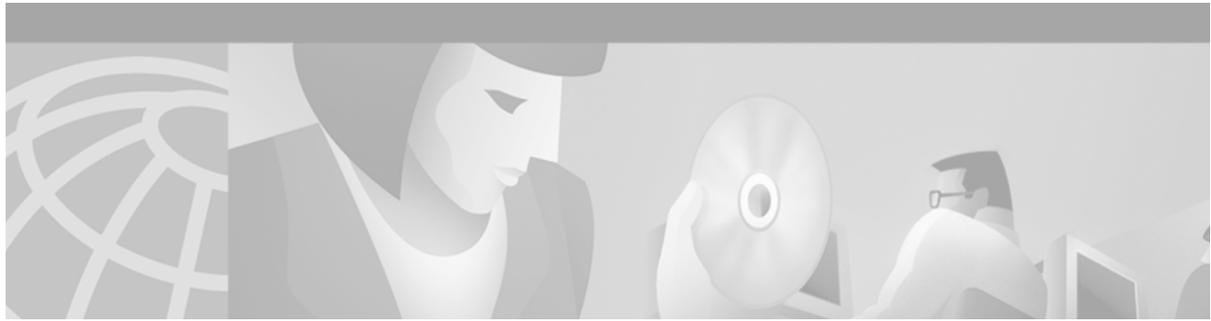
# show crypto map (IPSec)

To view the crypto map configuration, use the **show crypto map** EXEC command.

```
show crypto map [interface interface | tag map-name]
```

<b>Syntax Description</b>	<b>interface <i>interface</i></b> (Optional) Displays only the crypto map set applied to the specified interface.
	<b>tag <i>map-name</i></b> (Optional) Displays only the crypto map set with the specified <i>map-name</i> .

■ show crypto map (IPSec)



# Certification Authority Interoperability Commands

---

This chapter describes the function and syntax of the certification authority interoperability commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

## certificate

To manually add certificates, use the **certificate** command in certificate chain configuration mode. To delete your router's certificate or any registration authority certificates stored on your router, use the **no** form of this command.

**certificate** *certificate-serial-number*

**no certificate** *certificate-serial-number*

---

### Syntax Description

*certificate-serial-number* Serial number of the certificate to add or delete.

---

## crl optional

To allow other peers' certificates to still be accepted by your router even if the appropriate certificate revocation list (CRL) is not accessible to your router, use the **crl optional** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

**crl optional**

**no crl optional**

---

### Syntax Description

This command has no arguments or keywords.

## crl query

To query the certificate revocation list (CRL) published by the configured root with the Lightweight Directory Access Protocol (LDAP) URL, use the **crl query** trusted root configuration command. To remove the **crl query** LDAP URL, use the **no** form of this command.

```
crl query ldap-url
```

```
no crl query ldap-url
```

---

### Syntax Description

*ldap-url*

Specifies the LDAP URL published by the configured root; for example, `ldap://another_server`.

---

## crypto ca authenticate

To authenticate the certification authority (by getting the CA's certificate), use the **crypto ca authenticate** command in global configuration mode.

```
crypto ca authenticate name
```

---

### Syntax Description

*name*

Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command.

---

## crypto ca certificate chain

To enter the certificate chain configuration mode, use the **crypto ca certificate chain** command in global configuration mode. (You need to be in certificate chain configuration mode to delete certificates.)

```
crypto ca certificate chain name
```

---

### Syntax Description

*name*

Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto ca identity** command.

---

## crypto ca certificate query

To specify that certificates and certificate revocation lists (CRLs) should not be stored locally but retrieved from the certification authority when needed, use the **crypto ca certificate query** command in global configuration mode. This command puts the router into query mode. To cause certificates and CRLs to be stored locally (the default), use the **no** form of this command.

**crypto ca certificate query**

**no crypto ca certificate query**

---

**Syntax Description** This command has no arguments or keywords.

## crypto ca crl request

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto ca crl request** command in global configuration mode. Use this command only when your CA does not support a registration authority (RA).

**crypto ca crl request** *name*

---

**Syntax Description** *name* Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command.

---

## crypto ca enroll

To obtain your router's certificate(s) from the certification authority, use the **crypto ca enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

**crypto ca enroll** *name*

**no crypto ca enroll** *name*

---

**Syntax Description** *name* Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto ca identity** command.

---

## crypto ca identity

To declare the certification authority that your router should use, use the **crypto ca identity** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

**crypto ca identity** *name*

**no crypto ca identity** *name*

---

### Syntax Description

<i>name</i>	Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.) The CA might require a particular name, such as its domain name.
-------------	---

---

## crypto ca trusted-root

To configure a trusted root with a selected name, use the **crypto ca trusted-root** global configuration command. To deconfigure a trusted root, use the **no** form of this command.

**crypto ca trusted-root** *name*

**no crypto ca trusted-root** *name*

---

### Syntax Description

<i>name</i>	Creates a name for the trusted root.
-------------	--------------------------------------

---

## crypto key generate rsa (CA)

To generate RSA key pairs, use the **crypto key generate rsa** command in global configuration mode.

**crypto key generate rsa** [**usage-keys**]

---

### Syntax Description

<b>usage-keys</b>	(Optional) Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.
-------------------	---

---

## crypto key zeroize rsa

To delete all RSA keys from your router, use the **crypto key zeroize rsa** command in global configuration mode.

**crypto key zeroize rsa**

---

### Syntax Description

	This command has no arguments or keywords.
--	--

## enrollment mode ra

To turn on registration authority mode, use the **enrollment mode ra** command in ca-identity configuration mode. To turn off RA mode, use the **no** form of the command.

**enrollment mode ra**

**no enrollment mode ra**

---

**Syntax Description** This command has no arguments or keywords.

## enrollment retry count

To specify how many times a router will resend a certificate request, use the **enrollment retry-count** command in ca-identity configuration mode. To reset the retry count to the default of 0, which indicates an infinite number of retries, use the **no** form of the command.

**enrollment retry count** *number*

**no enrollment retry count**

---

**Syntax Description** *number* Specify how many times the router will resend a certificate request when the router does not receive a certificate from the CA from the previous request.  
Specify from 1 to 100 retries.

---

## enrollment retry period

To specify the wait period between certificate request retries, use the **enrollment retry period** command in ca-identity configuration mode. To reset the retry period to the default of 1 minute, use the **no** form of this command.

**enrollment retry period** *minutes*

**no enrollment retry period**

---

**Syntax Description** *minutes* Specify the number of minutes the router waits before resending a certificate request to the certification authority, when the router does not receive a certificate from the CA by the previous request.  
Specify from 1 to 60 minutes. By default, the router retries every 1 minute.

---

## enrollment url

To specify the certification authority location by naming the CA's URL, use the **enrollment url** command in ca-identity configuration mode. To remove the CA's URL from the configuration, use the **no** form of this command.

**enrollment url** *url*

**no enrollment url** *url*

---

### Syntax Description

*url*

Specify the URL of the CA where your router should send certificate requests, for example, http://ca\_server.

This URL must be in the form of http://CA\_name, where CA\_name is the CA's host Domain Name System name or IP address.

If the CA cgi-bin script location is not /cgi-bin/pkiclient.exe at the CA (the default CA cgi-bin script location) you need to also include the non-standard script location in the URL, in the form of http://CA\_name/script\_location where script\_location is the full path to the CA scripts.

---

## query url

To specify LDAP protocol support, use the **query url** command in ca-identity configuration mode. To remove the query URL from the configuration and specify the default query protocol, Simple Certificate Enrollment Protocol (SCEP), use the **no** form of this command.

**query url** *url*

**no query url** *url*

---

### Syntax Description

*url*

Specify the URL of the Lightweight Directory Access Protocol server; for example, ldap://another\_server.

This URL must be in the form of ldap://server\_name where server\_name is the host Domain Name System name or IP address of the LDAP server.

---

## root CEP

To define the Simple Certificate Enrollment Protocol (SCEP), which gets the root certificate of a given certification authority, use the **root CEP** trusted root configuration command.

**root CEP** *url*

---

### Syntax Description

*url*

Specifies the given URL of the configured root.

---

## root PROXY

To define the Hypertext Transfer Protocol proxy server for getting the root certificate, use the **root PROXY** trusted root configuration command.

**root PROXY** *url*

---

### Syntax Description

<i>url</i>	Specifies the URL of the HTTP proxy server; for example, <code>http://proxy_server</code> .
------------	---

---

## root TFTP

To define the TFTP protocol, which gets the root certificate of a given certification authority, use the **root TFTP** trusted root configuration command.

**root TFTP** *server-hostname filename*

---

### Syntax Description

<i>server-hostname</i>	Creates a name for the server.
<i>filename</i>	Creates a name for the file that will store the root certificate.

---

## show crypto ca certificates

To view information about your certificate, the certification authority certificate, and any registration authority certificates, use the **show crypto ca certificates** command in EXEC mode.

**show crypto ca certificates**

---

### Syntax Description

This command has no arguments or keywords.

## show crypto ca roots

To display the roots configured in the router, use the **show crypto ca roots** EXEC configuration command.

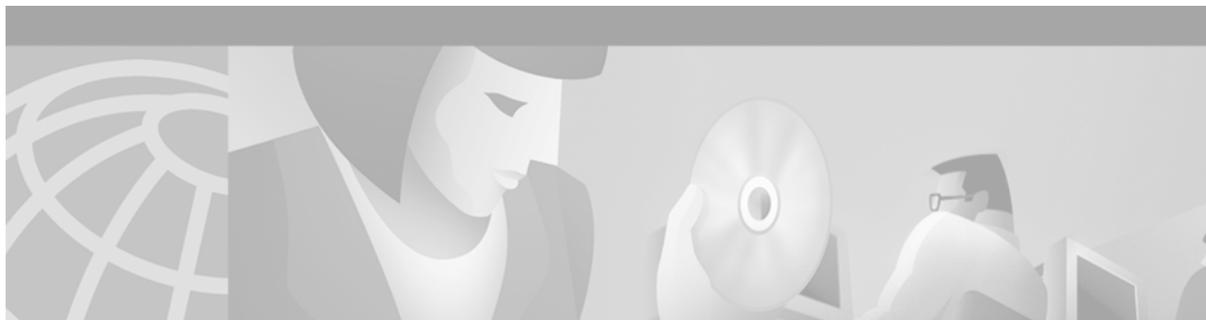
**show crypto ca roots**

---

### Syntax Description

This command has no arguments or keywords.

■ show crypto ca roots



## Internet Key Exchange Security Protocol Commands

---

This chapter describes the function and syntax of the Internet Key Exchange (IKE) security protocol commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### address

To specify the IP address of the remote peer's RSA public key you will manually configure, use the **address** public key configuration command.

**address** *ip-address*

---

#### Syntax Description

<i>ip-address</i>	Specifies the IP address of the remote peer.
-------------------	--

---

### addressed-key

To specify which peer's RSA public key you will manually configure, use the **addressed-key** public key chain configuration command.

**addressed-key** *key-address* [**encryption** | **signature**]

---

#### Syntax Description

<i>key-address</i>	Specifies the IP address of the remote peer's RSA keys.
<b>encryption</b>	(Optional) Indicates that the RSA public key to be specified will be an encryption special usage key.
<b>signature</b>	(Optional) Indicates that the RSA public key to be specified will be a signature special usage key.

---

## authentication (IKE policy)

To specify the authentication method within an Internet Key Exchange policy, use the **authentication** ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. To reset the authentication method to the default value, use the **no** form of this command.

**authentication** { *rsa-sig* | *rsa-encr* | *pre-share* }

**no authentication**

Syntax Description	Parameter	Description
	<b>rsa-sig</b>	Specifies RSA signatures as the authentication method.
	<b>rsa-encr</b>	Specifies RSA encrypted nonces as the authentication method.
	<b>pre-share</b>	Specifies preshared keys as the authentication method.

## clear crypto isakmp

To clear active Internet Key Exchange connections, use the **clear crypto isakmp** EXEC configuration command.

**clear crypto isakmp** [*connection-id*]

Syntax Description	Parameter	Description
	<i>connection-id</i>	(Optional) Specifies which connection to clear. If this argument is not used, all existing connections will be cleared.

## crypto isakmp client configuration address-pool local

To configure the IP address local pool to reference Internet Key Exchange on your router, use the **crypto isakmp client configuration address-pool local** global configuration command. To restore the default value, use the **no** form of this command.

**crypto isakmp client configuration address-pool local** *pool-name*

**no crypto isakmp client configuration address-pool local**

Syntax Description	Parameter	Description
	<i>pool-name</i>	Specifies the name of a local address pool.

## crypto isakmp enable

To globally enable Internet Key Exchange at your peer router, use the **crypto isakmp enable** global configuration command. To disable IKE at the peer, use the **no** form of this command.

```
crypto isakmp enable
no crypto isakmp enable
```

**Syntax Description** This command has no arguments or keywords.

## crypto isakmp identity

To define the identity used by the router when participating in the Internet Key Exchange protocol, use the **crypto isakmp identity** global configuration command. Set an Internet Security Association Key Management Protocol identity whenever you specify preshared keys. To reset the ISAKMP identity to the default value (address), use the **no** form of this command.

```
crypto isakmp identity {address | hostname}
no crypto isakmp identity
```

<b>Syntax Description</b>	<b>address</b>	Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations.
	<b>hostname</b>	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

## crypto isakmp key

To configure a preshared authentication key, use the **crypto isakmp key** global configuration command. You must configure this key whenever you specify preshared keys in an Internet Key Exchange policy. To delete a preshared authentication key, use the **no** form of this command.

```
crypto isakmp key keystring address peer-address [mask]
crypto isakmp key keystring hostname peer-hostname
no crypto isakmp key keystring address peer-address
no crypto isakmp key keystring hostname peer-hostname
```

<b>Syntax Description</b>	<b>address</b>	Use this keyword if the remote peer Internet Security Association Key Management Protocol identity was set with its IP address.
	<b>hostname</b>	Use this keyword if the remote peer ISAKMP identity was set with its host name.
	<i>keystring</i>	Specify the preshared key. Use any combination of alphanumeric characters up to 128 bytes. This preshared key must be identical at both peers.
	<i>peer-address</i>	Specify the IP address of the remote peer.

<i>peer-hostname</i>	Specify the host name of the remote peer. This is the peer's host name concatenated with its domain name (for example, myhost.example.com).
<i>mask</i>	(Optional) Specify the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)

## crypto isakmp policy

To define an Internet Key Exchange policy, use the **crypto isakmp policy** global configuration command. IKE policies define a set of parameters to be used during the IKE negotiation. To delete an IKE policy, use the **no** form of this command.

**crypto isakmp policy** *priority*

**no crypto isakmp policy**

<b>Syntax Description</b>	<i>priority</i>	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest.
---------------------------	-----------------	--

## crypto key generate rsa (IKE)

To generate RSA key pairs, use the **crypto key generate rsa** global configuration command.

**crypto key generate rsa** [*usage-keys*]

<b>Syntax Description</b>	<i>usage-keys</i>	(Optional) Specifies that two RSA special usage key pairs should be generated (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.
---------------------------	-------------------	---

## crypto key pubkey-chain rsa

To enter public key configuration mode (so you can manually specify other devices' RSA public keys), use the **crypto key pubkey-chain rsa** global configuration command.

**crypto key pubkey-chain rsa**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## crypto map client authentication list

To configure Internet Key Exchange extended authentication (Xauth) on your router, use the **crypto map client authentication list** global configuration command. To restore the default value, use the **no** form of this command.

**crypto map** *map-name* **client authentication list** *list-name*

**no crypto map** *map-name* **client authentication list** *list-name*

Syntax Description		
	<i>map-name</i>	The name you assign to the crypto map set.
	<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in. The list-name must match the list-name defined during AAA configuration.

## crypto map client configuration address

To configure IKE Mode Configuration on your router, use the **crypto map client configuration address** global configuration command. To disable IKE Mode Configuration, use the **no** form of this command.

**crypto map** *tag* **client configuration address** [**initiate** | **respond**]

**no crypto map** *tag* **client configuration address**

Syntax Description		
	<i>tag</i>	The name that identifies the crypto map.
	<b>initiate</b>	(Optional) A keyword that indicates the router will attempt to set IP addresses for each peer.
	<b>respond</b>	(Optional) A keyword that indicates the router will accept requests for IP addresses from any requesting peer.

## crypto map isakmp authorization list

To enable Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto map isakmp authorization list** global configuration command. To restore the default value, use the **no** form of this command.

**crypto map** *map-name* **isakmp authorization list** *list-name*

**no crypto map** *map-name* **isakmp authorization list** *list-name*

Syntax Description		
	<i>map-name</i>	Name you assign to the crypto map set.
	<i>list-name</i>	Character string used to name the list of authorization methods activated when a user logs in. The list name must match the list name defined during AAA configuration.

## encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange policy, use the **encryption** ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the **no** form of this command.

```
encryption { des | 3des }
```

```
no encryption
```

Syntax Description		
	<b>des</b>	Specifies 56-bit DES-CBC as the encryption algorithm.
	<b>3des</b>	Specifies 168-bit DES (3DES) as the encryption algorithm.

## group (IKE policy)

To specify the Diffie-Hellman group identifier within an Internet Key Exchange policy, use the **group** ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

```
group { 1 | 2 }
```

```
no group
```

Syntax Description		
	<b>1</b>	Specifies the 768-bit Diffie-Hellman group.
	<b>2</b>	Specifies the 1024-bit Diffie-Hellman group.

## hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the **hash** ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default SHA-1 hash algorithm, use the **no** form of this command.

```
hash { sha | md5 }
```

```
no hash
```

Syntax Description		
	<b>sha</b>	Specifies SHA-1 (HMAC variant) as the hash algorithm.
	<b>md5</b>	Specifies MD5 (HMAC variant) as the hash algorithm.

## key-string (IKE)

To manually specify a remote peer's RSA public key, use the **key-string** public key configuration command.

**key-string** *key-string*

<b>Syntax Description</b>	<i>key-string</i>	Enter the key in hexadecimal format. While entering the key data you can press Return to continue entering data.
---------------------------	-------------------	--

## lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange security association (SA), use the **lifetime** Internet Security Association Key Management Protocol policy configuration command. To reset the SA lifetime to the default value, use the **no** form of this command.

**lifetime** *seconds*

**no lifetime**

<b>Syntax Description</b>	<i>seconds</i>	Number of many seconds for each SA should exist before expiring. Use an integer from 60 to 86,400 seconds.
---------------------------	----------------	--

## named-key

To specify which peer's RSA public key you will manually configure, use the **named-key** public key chain configuration command. This command should only be used when the router has a single interface that processes IP Security.

**named-key** *key-name* [**encryption** | **signature**]

<b>Syntax Description</b>	<i>key-name</i>	Specifies the name of the remote peer's RSA keys. This is always the fully qualified domain name of the remote peer; for example, router.example.com.
	<b>encryption</b>	(Optional) Indicates that the RSA public key to be specified will be an encryption special-usage key.
	<b>signature</b>	(Optional) Indicates that the RSA public key to be specified will be a signature special-usage key.

## show crypto isakmp policy

To view the parameters for each Internet Key Exchange policy, use the **show crypto isakmp policy** EXEC command.

```
show crypto isakmp policy
```

---

**Syntax Description** This command has no arguments or keywords.

## show crypto isakmp sa

To view all current Internet Key Exchange security associations (SAs) at a peer, use the **show crypto isakmp sa** EXEC command.

```
show crypto isakmp sa
```

---

**Syntax Description** This command has no arguments or keywords.

## show crypto key mypubkey rsa

To view the RSA public keys of your router, use the **show crypto key mypubkey rsa** EXEC command.

```
show crypto key mypubkey rsa
```

---

**Syntax Description** This command has no arguments or keywords.

## show crypto key pubkey-chain rsa

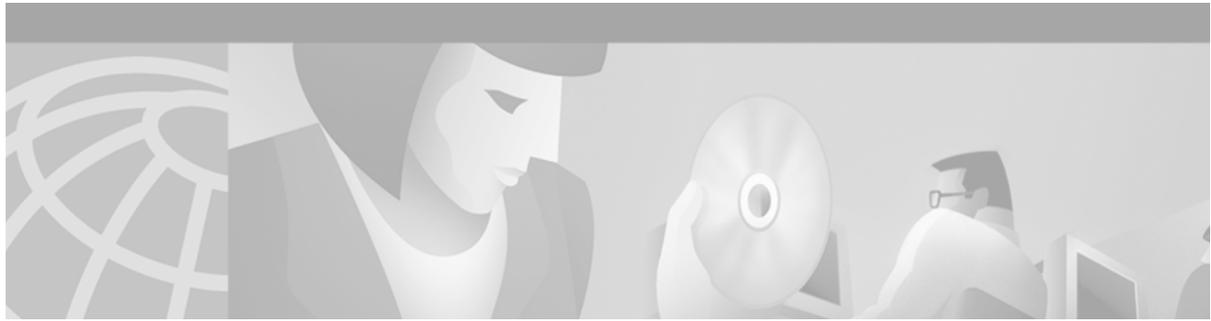
To view peers' RSA public keys stored on your router, use the **show crypto key pubkey-chain rsa** EXEC command.

```
show crypto key pubkey-chain rsa [name key-name | address key-address]
```

---

<b>Syntax Description</b>	<b>name</b> <i>key-name</i>	(Optional) The name of a particular public key to view.
	<b>address</b> <i>key-address</i>	(Optional) The address of a particular public key to view.

---



## Passwords and Privileges Commands

---

This chapter describes the function and syntax of the passwords and privileges commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove the password requirement use the **no** form of this command.

**enable password** [*level level*] {*password* | [*encryption-type*] *encrypted-password*}

**no enable password** [*level level*]

---

#### Syntax Description

<i>level level</i>	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the <b>no</b> form of the command, the privilege level defaults to 15 (traditional enable privileges).
<i>password</i>	Password users type to enter enable mode.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 7. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

## enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the **enable secret** function, use the **no** form of this command.

**enable secret** [*level level*] {*password* | [*encryption-type*] *encrypted-password*}

**no enable secret** [*level level*]

Syntax Description	level <i>level</i>	(Optional) Level for which the password applies. You can specify up to sixteen privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or in the <b>no</b> form of the command, the privilege level defaults to 15 (traditional enable privileges). The same holds true for the <b>no</b> form of the command.
	<i>password</i>	Password for users to enter enable mode. This password should be different from the password created with the <b>enable password</b> command.
	<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available for this command is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).
	<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

## password

To specify a password on a line, use the **password** command in line configuration mode. To remove the password, use the **no** form of this command.

**password** *password*

**no password**

Syntax Description	<i>password</i>	Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret.

# privilege level (global)

To set the privilege level for a command, use the **privilege level** command in configuration mode. To revert to default privileges for a given command, use the **no** form of this command.

**privilege mode** [*level level command* | **reset** *command*]

**no privilege mode level level command**

## Syntax Description

<i>mode</i>	Configuration mode. See Table 30 for a list of options for this argument.
<b>level</b>	(Optional) Enables setting a privilege level with a specified command.
<i>level</i>	(Optional) The privilege level associated with a command. You can specify up to sixteen privilege levels, using numbers 0 through 15.
<i>command</i>	(Optional) Command to which the privilege level is associated.
<b>reset</b>	(Optional) Resets the privilege level of a command.
<i>command</i>	(Optional) The command for which you want to reset the privilege level.

**Table 30 Mode Argument Options**

Command	Description
<b>accept-dialin</b>	VPDN group accept dialin configuration mode
<b>accept-dialout</b>	VPDN group accept dialout configuration mode
<b>address-family</b>	Address Family configuration mode
<b>atm-bm-config</b>	ATM bundle member configuration mode
<b>atm-bundle-config</b>	ATM bundle configuration mode
<b>atm-vc-config</b>	ATM virtual circuit configuration mode
<b>atmsig_e164_table_mode</b>	ATMSIG E164 Table
<b>cascustom</b>	Channel-associated signalling (cas) custom configuration mode
<b>configure</b>	Global configuration mode
<b>controller</b>	Controller configuration mode
<b>dhcp</b>	DHCP pool configuration mode
<b>dspfarm</b>	DSP farm configuration mode
<b>exec</b>	Exec mode
<b>flow-cache</b>	Flow aggregation cache configuration mode
<b>interface</b>	Interface configuration mode
<b>interface-dlci</b>	Frame Relay DLCI configuration mode
<b>ip-vrf</b>	Configure IP VRF parameters
<b>line</b>	Line configuration mode
<b>map-class</b>	Map class configuration mode
<b>map-list</b>	Map list configuration mode

**Table 30 Mode Argument Options (continued)**

<b>Command</b>	<b>Description</b>
<b>null-interface</b>	Null interface configuration mode
<b>preaut</b>	AAA Preauth definitions
<b>request-dialin</b>	VPDN group request dialin configuration mode
<b>request-dialout</b>	VPDN group request dialout configuration mode
<b>route-map</b>	Route map configuration mode
<b>router</b>	Router configuration mode
<b>tdm-conn</b>	TDM connection configuration mode
<b>vc-class</b>	VC class configuration mode
<b>vpdn-group</b>	VPDN group configuration mode
<b>rsvp_policy_local</b>	
<b>alps-ascu</b>	ALPS ASCU configuration mode
<b>alps-circuit</b>	ALPS circuit configuration mode
<b>config-rtr-http</b>	RTR HTTP raw request Configuration
<b>crypto-map</b>	Crypto map config mode
<b>crypto-transform</b>	Crypto transform config mode Crypto transform configuration mode
<b>gateway</b>	Gateway configuration mode
<b>ipenacl</b>	IP named extended access-list configuration mode
<b>ipsnacl</b>	IP named simple access-list configuration mode
<b>lane</b>	ATM Lan Emulation Leacs Configuration Table
<b>mpoa-client</b>	MPOA Client
<b>mpoa-server</b>	MPOA Server
<b>rtr</b>	RTR Entry Configuration
<b>sg-radius</b>	RADIUS server group definition
<b>sg-tacacs+</b>	TACACS+ server group
<b>sip-ua</b>	SIP UA configuration mode
<b>subscriber-policy</b>	Subscriber policy configuration mode
<b>tcl</b>	Tcl mode
<b>template</b>	Template configuration mode
<b>translation-rule</b>	Translation Rule configuration mode
<b>voiceclass</b>	Voice Class configuration mode
<b>voiceport</b>	Voice configuration mode
<b>voipdialpeer</b>	Dial Peer configuration mode

## privilege level (line)

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

**privilege level** *level*

**no privilege level**

---

**Syntax Description**

*level* Privilege level associated with the specified line.

---

## service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

**service password-encryption**

**no service password-encryption**

---

**Syntax Description**

This command has no arguments or keywords.

## show privilege

To display your current level of privilege, use the **show privilege** command in EXEC mode.

**show privilege**

---

**Syntax Description**

This command has no arguments or keywords.

## username

To establish a username-based authentication system, use the **username** command in global configuration mode.

**username** *name* { **nopassword** | **password** *password* | **password** *encryption-type*  
*encrypted-password* }

**username** *name* **password** *secret*

**username** *name* [**access-class** *number*]

**username** *name* [**autocommand** *command*]

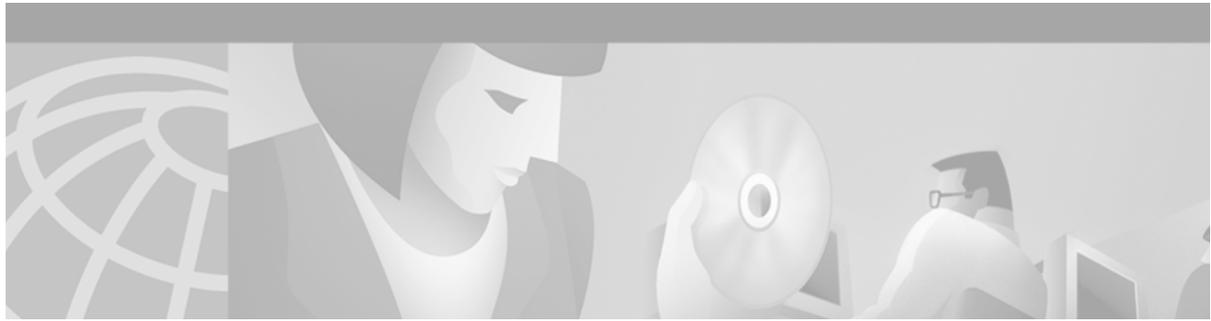
**username** *name* [**callback-dialstring** *telephone-number*]  
**username** *name* [**callback-rotary** *rotary-group-number*]  
**username** *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]  
**username** *name* **dnis**  
**username** *name* [**nocallback-verify**]  
**username** *name* [**noescape**] [**nohangup**]  
**username** *name* [**privilege** *level*]  
**username** *name* **user-maxlinks** *number*

**Syntax Description**

<i>name</i>	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
<b>nopassword</b>	No password is required for this user to log in. This is usually most useful in combination with the <b>autocommand</b> keyword.
<b>password</b>	Specifies a possibly encrypted password for this username.
<i>password</i>	Password a user enters.
<i>encryption-type</i>	Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
<i>encrypted-password</i>	Encrypted password a user enters.
<b>password</b>	Password to access the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the <b>username</b> command.
<i>secret</i>	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
<b>access-class</b>	(Optional) Specifies an outgoing access list that overrides the access list specified in the <b>access-class</b> line configuration command. It is used for the duration of the user's session.
<i>number</i>	(Optional) Access list number.
<b>autocommand</b>	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the <b>autocommand</b> keyword must be the last option on the line.
<i>command</i>	(Optional) The command string. Because the command can be any length and contain embedded spaces, commands using the <b>autocommand</b> keyword must be the last option on the line.

<b>callback-dialstring</b>	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
<i>telephone-number</i>	(Optional) For asynchronous callback only: telephone number to pass to the DCE device.
<b>callback-rotary</b>	(Optional) For asynchronous callback only: permits you to specify a rotary group number. The next available line in the rotary group is selected.
<i>rotary-group-number</i>	(Optional) For asynchronous callback only: integer between 1 and 100 that identifies the group of lines on which you want to enable a specific username for callback.
<b>callback-line</b>	(Optional) For asynchronous callback only: specific line on which you enable a specific username for callback.
<b>tty</b>	(Optional) For asynchronous callback only: standard asynchronous line.
<i>line-number</i>	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you want to enable a specific username for callback. Numbering begins with zero.
<i>ending-line-number</i>	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as <b>tty</b> ), then <i>line-number</i> and <i>ending-line-number</i> are absolute rather than relative line numbers.
<b>dnis</b>	Do not require password when obtained via DNIS.
<b>nocallback-verify</b>	(Optional) Authentication not required for EXEC callback on the specified line.
<b>noescape</b>	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
<b>nohangup</b>	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the <b>autocommand</b> keyword) has completed. Instead, the user gets another EXEC prompt.
<b>privilege</b>	(Optional) Sets the privilege level for the user.
<i>level</i>	(Optional) Number between 0 and 15 that specifies the privilege level for the user.
<b>user-maxlinks</b>	Limit the user's number of inbound links.
<i>number</i>	User-maxlinks limit for inbound links.

■ username



## IP Security Options Commands

---

This chapter describes the function and syntax of the IP security options commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### dnsix-dmdp retries

To set the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** command in global configuration mode. To restore the default number of retries, use the **no** form of this command.

**dnsix-dmdp retries** *count*

**no dnsix-dmdp retries** *count*

<b>Syntax Description</b>	<i>count</i>	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.
---------------------------	--------------	--

### dnsix-nat authorized-redirection

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** global configuration command. To delete an address, use the **no** form of this command.

**dnsix-nat authorized-redirection** *ip-address*

**no dnsix-nat authorized-redirection** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the host from which redirection requests are permitted.
---------------------------	-------------------	---

## dnsix-nat primary

To specify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat primary** command in global configuration mode. To delete an entry, use the **no** form of this command.

**dnsix-nat primary** *ip-address*

**no dnsix-nat primary** *ip-address*

---

### Syntax Description

<i>ip-address</i>	IP address for the primary collection center.
-------------------	---

---

## dnsix-nat secondary

To specify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat secondary** command in global configuration mode. To delete an entry, use the **no** form of this command.

**dnsix-nat secondary** *ip-address*

**no dnsix-nat secondary** *ip-address*

---

### Syntax Description

<i>ip-address</i>	IP address for the secondary collection center.
-------------------	---

---

## dnsix-nat source

To start the audit-writing module and to define the audit trail source address, use the **dnsix-nat source** command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the **no** form of this command.

**dnsix-nat source** *ip-address*

**no dnsix-nat source** *ip-address*

---

### Syntax Description

<i>ip-address</i>	Source IP address for DNSIX audit messages.
-------------------	---

---

## dnsix-nat transmit-count

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** command in global configuration mode. To revert to the default audit message count, use the **no** form of this command.

**dnsix-nat transmit-count** *count*

**no dnsix-nat transmit-count** *count*

---

### Syntax Description

<i>count</i>	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.
--------------	---

---

## ip security add

To add a basic security option to all outgoing packets, use the **ip security add** command in interface configuration mode. To disable the adding of a basic security option to all outgoing packets, use the **no** form of this command.

**ip security add**

**no ip security add**

---

### Syntax Description

This command has no arguments or keywords.

## ip security aeso

To attach Auxiliary Extended Security Options (AESOs) to an interface, use the **ip security aeso** command in interface configuration mode. To disable AESO on an interface, use the **no** form of this command.

**ip security aeso** *source compartment-bits*

**no ip security aeso** *source compartment-bits*

---

### Syntax Description

<i>source</i>	Extended Security Option (ESO) source. This can be an integer from 0 to 255.
<i>compartment-bits</i>	Number of compartment bits in hexadecimal.

---

## ip security dedicated

To set the level of classification and authority on the interface, use the **ip security dedicated** command in interface configuration mode. To reset the interface to the default classification and authorities, use the **no** form of this command.

**ip security dedicated** *level authority* [*authority...*]

**no ip security dedicated** *level authority* [*authority...*]

### Syntax Description

<i>level</i>	Degree of sensitivity of information. The <i>level</i> keywords are listed in Table 31.
<i>authority</i>	Organization that defines the set of security levels that will be used in a network. The <i>authority</i> keywords are listed in Table 32.

**Table 31** IPSO Level Keywords and Bit Patterns

Level Keyword	Bit Pattern
Reserved4	0000 0001
TopSecret	0011 1101
Secret	0101 1010
Confidential	1001 0110
Reserved3	0110 0110
Reserved2	1100 1100
Unclassified	1010 1011
Reserved1	1111 0001

**Table 32** IPSO Authority Keywords and Bit Patterns

Authority Keyword	Bit Pattern
Genser	1000 0000
Siop-Esi	0100 0000
DIA	0010 0000
NSA	0001 0000
DOE	0000 1000

## ip security eso-info

To configure system-wide defaults for extended IP Security Option (IPSO) information, use the **ip security eso-info** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**ip security eso-info** *source compartment-size default-bit*

**no ip security eso-info** *source compartment-size default-bit*

Syntax Description		
	<i>source</i>	Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 to 255.
	<i>compartment-size</i>	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 to 16.
	<i>default-bit</i>	Default bit value for any unspent compartment bits.

## ip security eso-max

To specify the maximum sensitivity level for an interface, use the **ip security eso-max** command in interface configuration mode. To return to the default, use the **no** form of this command.

**ip security eso-max** *source compartment-bits*

**no ip security eso-max** *source compartment-bits*

Syntax Description		
	<i>source</i>	Extended Security Option (ESO) source. This is an integer from 1 to 255.
	<i>compartment-bits</i>	Number of compartment bits in hexadecimal.

## ip security eso-min

To configure the minimum sensitivity for an interface, use the **ip security eso-min** command in interface configuration mode. To return to the default, use the **no** form of this command.

**ip security eso-min** *source compartment-bits*

**no ip security eso-min** *source compartment-bits*

Syntax Description		
	<i>source</i>	Extended Security Option (ESO) source. This is an integer from 1 to 255.
	<i>compartment-bits</i>	Number of compartment bits in hexadecimal.

## ip security extended-allowed

To accept packets on an interface that has an extended security option present, use the **ip security extended-allowed** command in interface configuration mode. To restore the default, use the **no** form of this command.

**ip security extended-allowed**

**no ip security extended-allowed**

---

**Syntax Description** This command has no arguments or keywords.

## ip security first

To prioritize the presence of security options on a packet, use the **ip security first** command in interface configuration mode. To prevent packets that include security options from moving to the front of the options field, use the **no** form of this command.

**ip security first**

**no ip security first**

---

**Syntax Description** This command has no arguments or keywords.

## ip security ignore-authorities

To have the Cisco IOS software ignore the authorities field of all incoming packets, use the **ip security ignore-authorities** command in interface configuration mode. To disable this function, use the **no** form of this command.

**ip security ignore-authorities**

**no ip security ignore-authorities**

---

**Syntax Description** This command has no arguments or keywords.

## ip security implicit-labelling

To force the Cisco IOS software to accept packets on the interface, even if they do not include a security option, use the **ip security implicit-labelling** command in interface configuration mode. To require security options, use the **no** form of this command.

**ip security implicit-labelling** [*level authority [authority...]*]

**no ip security implicit-labelling** [*level authority [authority...]*]

Syntax Description	
<i>level</i>	(Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. (See the <i>level</i> keywords listed in Table 31 in the <b>ip security dedicated</b> command section.)
<i>authority</i>	(Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. (See the <i>authority</i> keywords listed in Table 32 in the <b>ip security dedicated</b> command section.)

## ip security multilevel

To set the range of classifications and authorities on an interface, use the **ip security multilevel** command in interface configuration mode. To remove security classifications and authorities, use the **no** form of this command.

**ip security multilevel** *level1 [authority1...]* **to** *level2 authority2 [authority2...]*

**no ip security multilevel**

Syntax Description	
<i>level1</i>	Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. (See the <i>level</i> keywords found in Table 31 in the <b>ip security dedicated</b> command section.)
<i>authority1</i>	(Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. (See the <i>authority</i> keywords listed in Table 32 in the <b>ip security dedicated</b> command section.)
<b>to</b>	Separates the range of classifications and authorities.
<i>level2</i>	Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. (See the <i>level</i> keywords found in Table 31 in the <b>ip security dedicated</b> command section.)
<i>authority2</i>	Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. (See the <i>authority</i> keywords listed in Table 32 in the <b>ip security dedicated</b> command section.)

## ip security reserved-allowed

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the **ip security reserved-allowed** command in interface configuration mode. To disallow packets that have security levels of Reserved3 and Reserved2, use the **no** form of this command.

**ip security reserved-allowed**

**no ip security reserved-allowed**

---

**Syntax Description** This command has no arguments or keywords.

## ip security strip

To remove any basic security option on outgoing packets on an interface, use the **ip security strip** command in interface configuration mode. To restore security options, use the **no** form of this command.

**ip security strip**

**no ip security strip**

---

**Syntax Description** This command has no arguments or keywords.

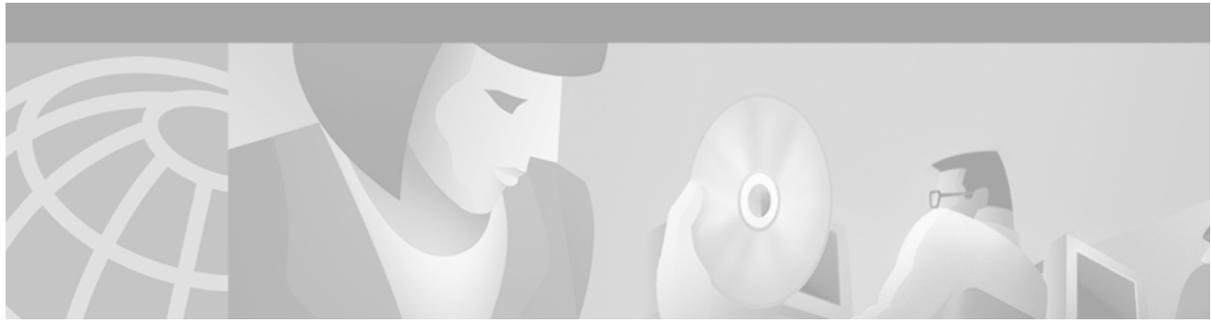
## show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the **show dnsix** command in privileged EXEC mode.

**show dnsix**

---

**Syntax Description** This command has no arguments or keywords.



## Unicast Reverse Path Forwarding Commands

---

This chapter describes the function and syntax of the Unicast Reverse Path Forwarding (Unicast RPF) command. For more information about this command, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### ip verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reverse-path** interface configuration command. To disable Unicast RPF, use the **no** form of this command.

**ip verify unicast reverse-path** *list*

**no ip verify unicast reverse-path**

---

**Syntax Description**

*list*

Specifies a numbered access control list (ACL) in the following ranges:

- 1 to 99 (IP standard access list)
  - 100 to 199 (IP extended access list)
  - 1300 to 1999 (IP standard access list, expanded range)
  - 2000 to 2699 (IP extended access list, expanded range)
-

■ ip verify unicast reverse-path



## Secure Shell Commands

---

This chapter describes the function and syntax of the Secure Shell (SSH) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Security Command Reference*.

### disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the **disconnect ssh** privileged EXEC command.

```
disconnect ssh [vtty] session-id
```

---

#### Syntax Description

<b>vtty</b>	(Optional) Virtual terminal for remote console access.
<i>session-id</i>	The session-id is the number of connection displayed in the <b>show ip ssh</b> command output.

---

### ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** global configuration command. To restore the default value, use the **no** form of this command.

```
ip ssh {[timeout seconds]} | [authentication-retries integer]
```

```
no ip ssh {[timeout seconds]} | [authentication-retries integer]
```

---

#### Syntax Description

<b>timeout</b>	(Optional) The time interval that the router waits for the SSH client to respond.  This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0–4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
<b>authentication-retries</b>	(Optional) The number of attempts after which the interface is reset.

---

<i>seconds</i>	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
<i>integer</i>	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

## show ip ssh

To display the version and configuration data for Secure Shell (SSH), use the **show ip ssh** privileged EXEC command.

```
show ip ssh
```

**Syntax Description** This command has no arguments or keywords.

## show ssh

To display the status of Secure Shell (SSH) server connections, use the **show ssh** privileged EXEC command.

```
show ssh
```

**Syntax Description** This command has no arguments or keywords.

## ssh

To start an encrypted session with a remote networking device, use the **ssh** user EXEC command.

```
ssh [-l userid] [-c {des | 3des}] [-o numberofpasswdprompts n] [-p portnum] {ipaddr | hostname}  
[command]
```

<b>Syntax Description</b>	<b>-l <i>userid</i></b>	(Optional) Specifies the user ID to use when logging in as on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.
	<b>-c {<b>des</b>   <b>3des</b>}</b>	(Optional) Specifies the crypto algorithm, DES or 3DES, to use for encrypting data. To use SSH, you must have an encryption image must be running on the router. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES).

---

<b>-o <code>numberofpasswdprompts</code> <i>n</i></b>	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the <b>-o <code>numberofpasswdprompts</code></b> keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
<b>-p <i>portnum</i></b>	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
<i>ipaddr</i>   <i>hostname</i>	Specifies the IP address or host name of the remote networking device.
<i>command</i>	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.

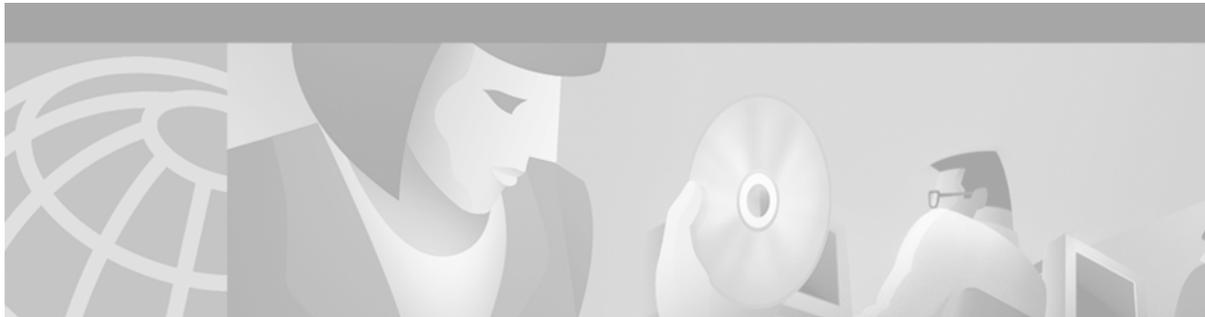
---





## **Interface**





## Interface Commands: **aps authenticate** Through interface **ctunnel**

---

This chapter describes the function and syntax of the interface commands: **aps authenticate** through **interface ctunnel**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Interface Command Reference*.

### **aps authenticate**

To enable authentication and specify the string that must be present to accept any packet on the out-of-band (OOB) communications channel on a packet-over-SONET (POS) interface, use the **aps authenticate** command in interface configuration mode. To disable authentication, use the **no** form of this command.

**aps authenticate** *string*

**no aps authenticate**

---

#### **Syntax Description**

<i>string</i>	Text that must be present to accept the packet on a protected or working interface. A maximum of eight alphanumeric characters are accepted.
---------------	--

---

### **aps force**

To manually switch the specified circuit to a protect interface, unless a request of equal or higher priority is in effect, use the **aps force** command in interface configuration mode. To cancel the switch, use the **no** form of this command.

**aps force** *circuit-number*

**no aps force** *circuit-number*

---

#### **Syntax Description**

<i>circuit-number</i>	Number of the circuit to switch to the protect interface.
-----------------------	---

---

## aps group

To allow more than one protect and working interface to be supported on a router, use the **aps group** command in interface configuration mode. To remove a group, use the **no** form of this command.

**aps group** *group-number*

**no aps group** *group-number*

Syntax Description	<i>group-number</i>	Number of the group.
--------------------	---------------------	----------------------

## aps lockout

To prevent a working interface from switching to a protect interface, use the **aps lockout** command in interface configuration mode. To remove the lockout, use the **no** form of this command.

**aps lockout** *circuit-number*

**no aps lockout** *circuit-number*

Syntax Description	<i>circuit-number</i>	Number of the circuit to lock out.
--------------------	-----------------------	------------------------------------

## aps manual

To manually switch a circuit to a protect interface, use the **aps manual** command in interface configuration mode. To cancel the switch, use the **no** form of this command.

**aps manual** *circuit-number*

**no aps manual** *circuit-number*

Syntax Description	<i>circuit-number</i>	Number of the circuit to switch to a protect interface.
--------------------	-----------------------	---

## aps protect

To enable a POS interface as a protect interface, use the **aps protect** command in interface configuration mode. To remove the POS interface as a protect interface, use the **no** form of this command.

**aps protect** *circuit-number ip-address*

**no aps protect** *circuit-number ip-address*

**Syntax Description**

<i>circuit-number</i>	Number of the circuit to enable as a protect interface.
<i>ip-address</i>	IP address of the router that has the working POS interface.

## aps revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **aps revert** command in interface configuration mode. To disable automatic switchover, use the **no** form of this command.

**aps revert** *minutes*

**no aps revert**

**Syntax Description**

<i>minutes</i>	Number of minutes until the circuit is switched back to the working interface after the working interface is available.
----------------	---

## aps timers

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **aps timers** command in interface configuration mode. To return to the default timers, use the **no** form of this command.

**aps timers** *seconds1 seconds2*

**no aps timers**

**Syntax Description**

<i>seconds1</i>	Number of seconds to wait before sending a hello packet (hello timer).
<i>seconds2</i>	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer).

## aps unidirectional

To configure a protect interface for unidirectional mode, use the **aps unidirectional** command in interface configuration mode. To return to the default, bidirectional mode, use the **no** form of this command.

**aps unidirectional**

**no aps unidirectional**

**Syntax Description**

This command has no arguments or keywords.

## aps working

To configure a Packet over SONET (POS) interface as a working interface, use the **aps working** command in interface configuration mode. To remove the protect option from the POS interface, use the **no** form of this command.

**aps working** *circuit-number*

**no aps working** *circuit-number*

---

### Syntax Description

<i>circuit-number</i>	Circuit number associated with this working interface.
-----------------------	--

---

## atm sonet

To set the mode of operation and thus control the type of the ATM cell used for cell-rate decoupling on the SONET physical layer interface module (PLIM), use the **atm sonet** command in interface configuration mode. To restore the default Synchronous Transport Signal level 12, concatenated (STS-12c) operation, use the **no** form of this command.

**atm sonet** [**stm-4**]

**no atm sonet** [**stm-4**]

---

### Syntax Description

<b>stm-4</b>	(Optional) Synchronous Digital Hierarchy/Synchronous Transport Signal level 4 (SDH/STM-4) operation (ITU-T specification).
--------------	--

---

## auto-polarity

To enable automatic receiver polarity reversal on a hub port connected to an Ethernet interface of a Cisco 2505 or Cisco 2507 router, use the **auto-polarity** command in hub configuration mode. To disable this feature, use the **no** form of this command.

**auto-polarity**

**no auto-polarity**

---

### Syntax Description

This command has no arguments or keywords.

## bandwidth (interface)

To set a bandwidth value for an interface, use the **bandwidth** command in interface configuration mode. To restore the default values, use the **no** form of this command.

**bandwidth** *kilobits*

**no bandwidth**

<b>Syntax Description</b>	<i>kilobits</i>	Intended bandwidth, in kilobits per second. For a full bandwidth DS3, enter the value 44736.
---------------------------	-----------------	--

## bert abort

To end a bit error rate testing session, use the **bert abort** command in privileged EXEC mode.

**bert abort**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## bert controller

To start a bit error rate test for a particular port, use the **bert controller** command in privileged EXEC mode.

**bert controller** [*type-controller*] [{*last-controller*} | **profile** [*number* | **default**]]

<b>Syntax Description</b>	<i>type-controller</i>	(Optional) Use either T1 or E1 depending on the type of facility.
	<i>last-controller</i>	(Optional) Last controller number. The valid range is 0 to 7.
	<b>profile</b>	Sets the profile numbers for the bit error rate test. The default is 0.
	<i>number</i>	(Optional) Numbers of the test profiles to use. The valid range is 0 to 15.
	<b>default</b>	(Optional) Executes the default bit error rate test (0).

## bert pattern

To enable a bit error rate (BER) test pattern on a T1 or E1 line, use the **bert pattern** command in controller configuration mode. To disable a BER test pattern, use the **no** form of this command.

```
bert pattern {2^23 | 2^20 | 2^20-QRSS | 2^15 | 2^11 | 1s | 0s | alt-0-1} interval time
```

```
no bert pattern {2^23 | 2^20 | 2^20-QRSS | 2^15 | 2^11 | 1s | 0s | alt-0-1} interval time
```

### Syntax Description

{ 2^23   2^20-QRSS   2^15   2^11   1s   0s   alt-0-1 }	<p>Specifies the length of the repeating BER test pattern. Values are:</p> <ul style="list-style-type: none"> <li>• <b>2^23</b>—Pseudorandom 0.151 test pattern that is 8,388,607 bits in length.</li> <li>• <b>2^20</b>—Pseudo-random 0.153 test pattern that is 1,048,575 bits in length.</li> <li>• <b>2^20-QRSS</b>—Pseudorandom quasi-random signal sequence (QRSS) 0.151 test pattern that is 1,048,575 bits in length.</li> <li>• <b>2^15</b>—Pseudorandom 0.151 test pattern that is 32,768 bits in length.</li> <li>• <b>2^11</b>—Pseudorandom test pattern that is 2,048 bits in length.</li> <li>• <b>1s</b>—Repeating pattern of ones (...111...).</li> <li>• <b>0s</b>—Repeating pattern of zeros (...000...).</li> <li>• <b>alt-0-1</b>—Repeating pattern of alternating zeros and ones (...01010...).</li> </ul>
interval time	<p>Specifies the duration of the BER test. The interval can be a value from 1 to 1440 minutes.</p>

## bert profile

To set up various bit error rate testing profiles, use the **bert profile** command in privileged EXEC mode. To disable the particular bit error rate test (BERT) profile indicated by profile number, use the **no** form of this command.

```
bert profile number pattern pattern threshold threshold error-injection err_inj duration time
```

```
no bert profile number pattern pattern threshold threshold error-injection err_inj duration time
```

### Syntax Description

number	<p>BERT profile number. The valid range is 1 to 15. This is the number assigned to a particular set of parameters. If no such profile of the same number exists in the system, a new profile is created with that number; otherwise, an existing set of parameters with that profile number is overwritten by the new profile.</p>
pattern	<p>Pattern that BERT will generate on the line.</p>

<i>pattern</i>	0s—repetitive pattern, all zeroes 1_in_16— <i>n</i> repetitive pattern, 1 in 16 1s— <i>n</i> repetitive pattern, all ones 211-O.152— <i>n</i> pseudo-random pattern, $2^{11} - 1$ O.152 215-O.15— <i>n</i> pseudo-random pattern, $2^{15} - 1$ O.151 220-O.151QRSS— <i>n</i> pseudo-random pattern, $2^{20} - 1$ O.151 QRSS (This is the default) 220-O.153— <i>n</i> pseudo-random pattern, $2^{20} - 1$ O.153 3_in_24— <i>n</i> repetitive pattern, 3 in 24
<b>threshold</b>	Test failure (error) threshold that determines if the BERT on this line passed.
<i>threshold</i>	10 <sup>-2</sup> —bit error rate of $10^{-2}$ 10 <sup>-3</sup> —bit error rate of $10^{-3}$ 10 <sup>-4</sup> —bit error rate of $10^{-4}$ 10 <sup>-5</sup> —bit error rate of $10^{-5}$ 10 <sup>-6</sup> —bit error rate of $10^{-6}$ (This is the default) 10 <sup>-7</sup> —bit error rate of $10^{-7}$ 10 <sup>-8</sup> —bit error rate of $10^{-8}$
<b>error-injection</b>	Error injection rate for bit errors injected into the BERT pattern generated by the chip. The default is none.
<i>err_inj</i>	10 <sup>-1</sup> —Error injection of $10^{-1}$ 10 <sup>-2</sup> —Error injection of $10^{-2}$ 10 <sup>-3</sup> —Error injection of $10^{-3}$ 10 <sup>-4</sup> —Error injection of $10^{-4}$ 10 <sup>-5</sup> —Error injection of $10^{-5}$ 10 <sup>-6</sup> —Error injection of $10^{-6}$ 10 <sup>-7</sup> —Error injection of $10^{-7}$ none—No error injection in the data pattern.
<b>duration</b>	Duration, in minutes, for which BERT is to be executed.
<i>time</i>	Duration of BERT, in minutes. The valid range is 1 to 1440. The default is 10.

## cablelength

To specify the distance of the cable from the routers to the network equipment, use the **cablelength** command in controller configuration mode. To restore the default cable length, use the **no** form of this command.

**cablelength** *feet*

**no cablelength**

### Syntax Description

<i>feet</i>	Number of feet in the range of 0 to 450. The default values are: <ul style="list-style-type: none"> <li>• 224 feet for Channelized T3 Interface Processor (CT3IP)</li> <li>• 49 feet for PA-T3 and PA-2T3 port adapters</li> </ul>
-------------	--

## cablelength long

To increase the pulse of a signal at the receiver and decrease the pulse from the transmitter using pulse equalization and line build-out for a T1 cable, use the **cablelength long** command in controller configuration or interface configuration mode. To return the pulse equalization and line build-out values to their default settings, use the **no** form of this command.

**cablelength long** *dbgain-value dbloss-value*

**no cablelength long**

Syntax Description		
	<i>dbgain-value</i>	Number of decibels (dB) by which the receiver signal is increased. Use one of the following values: <ul style="list-style-type: none"> <li>• gain26</li> <li>• gain36</li> </ul> The default is 26 dB.
	<i>dbloss-value</i>	Number of decibels by which the transmit signal is decreased. Use one of the following values: <ul style="list-style-type: none"> <li>• 0db</li> <li>• -7.5db</li> <li>• -15db</li> <li>• -22.5db</li> </ul> The default is 0 dB.

## cablelength short

To set a cable length 655 feet or shorter for a DS1 link on the Cisco MC3810 or Cisco 2600 and 3600 series routers, use the **cablelength short** command in controller configuration or interface configuration mode. This command is supported on T1 controllers only. To delete the **cablelength short** value, use the **no** form of this command. To set cable lengths longer than 655 feet, use the **cablelength long** command.

**cablelength short** *length*

**no cablelength short**

Syntax Description		
	<i>length</i>	Specifies a cable length. Use one of the following values to specify this value: <ul style="list-style-type: none"> <li>• 133—Specifies a cable length from 0 to 133 feet.</li> <li>• 266—Specifies a cable length from 134 to 266 feet.</li> <li>• 399—Specifies a cable length from 267 to 399 feet.</li> <li>• 533—Specifies a cable length from 400 to 533 feet.</li> <li>• 655—Specifies a cable length from 534 to 655 feet.</li> </ul>

## carrier-delay

To set the carrier delay on a serial interface, use the **carrier-delay** command in interface configuration mode. To return to the default carrier delay value, use the **no** form of this command.

**carrier-delay** [*seconds*]

**no carrier-delay** [*seconds*]

<b>Syntax Description</b>	<i>seconds</i> (Optional) Time, in seconds, to wait for the system to change states. Enter an integer in the range 0 to 60. The default is 2 seconds.
---------------------------	---

## channel-group (Fast EtherChannel)

To assign a Fast Ethernet interface to a Fast EtherChannel group, use the **channel-group** command in interface configuration mode. To remove a Fast Ethernet interface from a Fast EtherChannel group, use the **no** form of this command.

**channel-group** *channel-number*

**no channel-group** *channel-number*

<b>Syntax Description</b>	<i>channel-number</i> Port-channel number previously assigned to the port-channel interface when using the <b>interface port-channel</b> global configuration command. The range is 1 to 4.
---------------------------	---

## clear aim

To clear data compression of the Advanced Interface Module (AIM) daughtercard registers and reset the hardware, use the **clear aim** command in privileged EXEC mode.

**clear aim** *element-number*

<b>Syntax Description</b>	<i>element-number</i> Enables compression for this AIM slot. AIM slots begin with 0.
---------------------------	--

## clear controller lex

To reboot the LAN Extender chassis and restart its operating software, use the **clear controller lex** command in privileged EXEC mode.

**clear controller lex** *number* [**prom**]

### Cisco 7500 Series

**clear controller lex** *slot/port* [**prom**]

**Cisco 7200 Series and 7500 Series with a Packet over SONET Interface Processor**

```
clear controller lex [type] slot/port
```

**Cisco 7500 Series with Ports on VIP Cards**

```
clear controller lex [type] slot/port-adapter/port
```

**Syntax Description**

<i>number</i>	Number of the LAN Extender interface corresponding to the LAN Extender to be rebooted.
<b>prom</b>	(Optional) Forces a reload of the PROM image, regardless of any Flash image.
<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>type</i>	(Optional) Specifies the interface type. See Table 33 under the <b>clear counters</b> command for keywords.
<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## clear counters

To clear the interface counters, use the **clear counters** command in user EXEC mode.

```
clear counters [type number]
```

**Cisco 4000 Series or Cisco 7500 Series with a LAN Extender Interface**

```
clear counters [type slot/port] [ethernet | serial]
```

**Cisco 7200 Series and 7500 Series with a Packet over SONET Interface Processor**

```
clear counters [type] slot/port
```

**Cisco 7500 Series with Ports on VIP Cards**

```
clear counters [type] slot/port-adapter/port
```

**Syntax Description**

<i>type</i>	(Optional) Specifies the interface type; one of the keywords listed in Table 33.
<i>number</i>	(Optional) Specifies the interface counter displayed with the <b>show interfaces</b> command.
<b>ethernet</b>	(Optional) If the <i>type</i> is <b>lex</b> , you can clear the interface counters on the Ethernet interface.
<b>serial</b>	(Optional) If the <i>type</i> is <b>lex</b> , you can clear the interface counters on the serial interface.

<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

**Table 33** *clear counters Interface Type Keywords*

<b>Keyword</b>	<b>Interface Type</b>
<b>async</b>	Asynchronous interface
<b>bri</b>	ISDN BRI
<b>dialer</b>	Dialer interface
<b>ethernet</b>	Ethernet interface
<b>fast-ethernet</b>	Fast Ethernet interface
<b>fddi</b>	FDDI
<b>hssi</b>	High-Speed Serial Interface (HSSI)
<b>lex</b>	LAN Extender interface
<b>loopback</b>	Loopback interface
<b>null</b>	Null interface
<b>port-channel</b>	Port channel interface
<b>pos</b>	Packet OC-3 interface
<b>serial</b>	Synchronous serial interface
<b>switch</b>	Switch interface
<b>tokenring</b>	Token Ring interface
<b>tunnel</b>	Tunnel interface
<b>vg-anylan</b>	100VG-AnyLAN port adapter

## clear hub

To reset and reinitialize the hub hardware connected to an interface of a Cisco 2505 or Cisco 2507 router, use the **clear hub** command in EXEC mode.

**clear hub ethernet** *number*

### Syntax Description

<b>ethernet</b>	Hub in front of an Ethernet interface.
<i>number</i>	Hub number to clear, starting with 0. Because there is only one hub, this number is 0.

## clear hub counters

To set to zero the hub counters on an interface of a Cisco 2505 or Cisco 2507 router, use the **clear hub counters** command in EXEC mode.

```
clear hub counters [ether number [port [end-port]]]
```

Syntax	Description
<b>ether</b>	(Optional) Hub in front of an Ethernet interface.
<i>number</i>	(Optional) Hub number for which to clear counters. Because there is currently only one hub, this number is 0. If you specify the keyword <b>ether</b> , you must specify the <i>number</i> .
<i>port</i>	(Optional) Port number on the hub. On the Cisco 2505 router, port numbers range from 1 to 8. On the Cisco 2507 router, port numbers range from 1 to 16. If a second port number follows, this port number indicates the beginning of a port range. If you do not specify a port number, counters for all ports are cleared.
<i>end-port</i>	(Optional) Ending port number of a range.

## clear interface

To reset the hardware logic on an interface, use the **clear interface** command in EXEC mode.

```
clear interface type number [name-tag]
```

### Cisco 7200 Series and Cisco 7500 Series with a Packet OC-3 Interface Processor

```
clear interface type slot/port
```

### Cisco 7500 Series with Ports on VIP Cards

```
clear interface type slot/port-adapter/port
```

### Cisco 7500 Series

```
clear interface type slot/port [:channel-group]
```

### Cisco 7500 Series with a CT3IP

```
clear interface type slot/port-adapter/port [:t1-channel]
```

Syntax	Description
<i>type</i>	Interface type; it is one of the keywords listed in Table 34.
<i>number</i>	Port, connector, or interface card number.
<i>name-tag</i>	(Optional) Logic name to identify the server configuration so that multiple entries of server configuration can be entered.  This optional argument is for use with the RLM feature.
<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.

<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
<i>:channel-group</i>	(Optional) On Cisco 7500 series routers supporting channelized T1, specifies the channel from 0 to 23. This number is preceded by a colon.
<i>:t1-channel</i>	(Optional) For the CT3IP, the T1 channel is a number between 1 and 28.  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 ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

**Table 34** *clear interface Type Keywords*

<b>Keyword</b>	<b>Interface Type</b>
<b>async</b>	Async interface
<b>atm</b>	ATM interface
<b>bri</b>	ISDN BRI
<b>ethernet</b>	Ethernet interface
<b>fdi</b>	FDDI
<b>hssi</b>	High-Speed Serial Interface (HSSI)
<b>loopback</b>	Loopback interface
<b>null</b>	Null interface
<b>port-channel</b>	Port channel interface
<b>pos</b>	Packet OC-3 Interface Processor
<b>serial</b>	Synchronous serial interface
<b>switch</b>	Switch interface
<b>tokenring</b>	Token Ring interface
<b>tunnel</b>	Tunnel interface
<b>vg-anylan</b>	100VG-AnyLAN port adapter

## clear interface fastethernet

To reset the controller for a specified Fast Ethernet interface, use the **clear interface fastethernet** command in privileged EXEC mode.

### Cisco 4500 and 4700 series

```
clear interface fastethernet number
```

### Cisco 7200 and 7500 series

```
clear interface fastethernet slot/port
```

**Cisco 7500 series**

```
clear interface fastethernet slot/port-adapter/port
```

Syntax Description		
	<i>number</i>	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
	<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	Number of the port-adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## clear interface serial

To reset the statistical information specific to a serial interface, use the **clear interface serial** command in user EXEC mode.

```
clear interface serial dial-shelf/slot/t3-port:t1-num:chan-group
```

Syntax Description		
	<i>dial-shelf</i>	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
	<i>slot</i>	Location of the CT3 interface card in the dial shelf chassis.
	<i>t3-port</i>	T3 port number. The only valid value is 0.
	<i>:t1-num</i>	T1 timeslot in the T3 line. The value can be from 1 to 28.
	<i>:chan-group</i>	Channel group identifier.

## clear service-module serial

To reset an integrated CSU/DSU, use the **clear service-module serial** command in privileged EXEC configuration mode.

```
clear service-module serial number
```

Syntax Description		
	<i>number</i>	Number of the serial interface.

## clock rate

To configure the clock rate for the hardware connections on serial interfaces such as network interface modules (NIMs) and interface processors to an acceptable bit rate, use the **clock rate** command in interface configuration mode. 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.

**clock rate** *bps*

**no clock rate**

<b>Syntax Description</b>	<p><i>bps</i> Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000.</p> <p>For the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+), a nonstandard clock rate can be used. You can enter any value from 300 to 8000000 bps. The clock rate you enter is rounded (adjusted), if necessary, to the nearest value your hardware can support except for the following standard rates: 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 56000, 64000, 128000, or 2015232.</p> <p>The default is no clock rate configured.</p>
---------------------------	---

## clock source

To configure the clock source of a DS1 link, enter the **clock source** command in interface configuration, controller configuration, or ATM interface configuration mode. To restore the default **line** setting, use the **no** form of this command.

**clock source** {**line** | **internal** | **loop-timed**}

**no clock source**

<b>Syntax Description</b>	<p><b>line</b> Specifies that the T1/E1 link uses the recovered clock from the line. This is the default.</p> <p><b>internal</b> Specifies that the T1/E1 link uses the internal clock from the interface.</p> <p><b>loop-timed</b> Specifies that the T1/E1 interface takes the clock from the Rx (line) and uses it for Tx.</p>
---------------------------	---

## clock source (AS5200)

To select the clock source for the time-division multiplexing (TDM) bus in a Cisco AS5200 access server, use the **clock source** command in interface configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

**clock source** {**line** {**primary** | **secondary**} | **internal**}

**no clock source line** {**primary** | **secondary**}

Syntax Description	line	Clock source on the active line.
	<b>primary</b>	Primary TDM clock source.
	<b>secondary</b>	Secondary TDM clock source.
	<b>internal</b>	Selects the free running clock (also known as internal clock) as the clock source.

## clock source (controller)

To set the T1-line clock source for the Multichannel Interface Processor (MIP) in the Cisco 7200 series and Cisco 7500 series, the NPM in the Cisco 4000 series, a T3 interface, or a PA-T3 serial port adapter, use the **clock source** command in controller configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

```
clock source {line {primary | secondary} | internal}
```

```
no clock source
```

Syntax Description	line	Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream. This is the default.
	<b>primary</b>	Specifies the source of primary line clocking. The default primary TDM clock source is from the T0 controller.
	<b>secondary</b>	Specifies the source of secondary line clocking. The default secondary TDM clock source is from the T1 controller.
	<b>internal</b>	Specifies that the interface will clock its transmitted data from its internal clock.

## clock source (CT3IP)

To specify where the clock source is obtained for use by the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **clock source** command in controller configuration mode. To restore the default clock source, use the **no** form of this command.

```
clock source {internal | line | loop-timed}
```

```
no clock source
```

	<b>internal</b>	Specifies that the internal clock source is used. This is the default.
	<b>line</b>	Specifies that the network clock source is used.
	<b>loop-timed</b>	Decouples the controller clock from the system-wide clock set with the <b>network-clock-select</b> command. The loop-timed clock enables the Digital Voice Module (DVM) to connect to a PBX and to connect the multiflex trunk module (MFT) to a central office when both the PBX and the central office function as DCE clock sources. This situation assumes that the PBX also takes the clocking from the central office, thereby synchronizing the clocks on the DVM and the MFT.

## clock source (interface)

To control the clock from which a G.703-E1 interface, an E1-G.703/G.704 serial port adapter, or a PA-E3 serial port adapter clocks its transmitted data, use the **clock source** command in interface configuration mode. To restore the default clock source, use the **no** form of this command.

### Cisco 4000, 7000, 7200, and 7500 Series

**clock source** { **line** | **internal** }

**no clock source**

### Cisco AS5200 and AS5300 Access Servers

**clock source** { **line** { **primary** | **secondary** } | **internal** }

**no clock source line** { **primary** | **secondary** }

#### Syntax Description

<b>line</b>	Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream. This is the default.
<b>internal</b>	Specifies that the interface will clock its transmitted data from its internal clock.
<b>primary</b>	Primary time-division multiplexing (TDM) clock source.
<b>secondary</b>	Secondary TDM clock source.

## clock source (MC3810)

To specify the clock source of a DS1 link on the Cisco MC3810 multiservice access concentrator, use the **clock source** command in controller configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

**clock source** { **line** | **internal** | **loop-timed** }

**no clock source**

#### Syntax Description

<b>line</b>	Specifies that the DS1 link uses the recovered clock. The line value is the default clock source used when the Multiflex Trunk (MFT) is installed.
<b>internal</b>	Specifies that the DS1 link uses the internal clock. The internal value is the default clock source used when the Digital Voice Module (DVM) is installed.
<b>loop-timed</b>	Specifies that the T1/E1 controller will take the clock from the Rx (line) and use it for Tx. This setting decouples the controller clock from the system-wide clock set with the <b>network-clock-select</b> command. The loop-timed clock enables the DVM to connect to a PBX and to connect the MFT to a central office when both the PBX and the central office function as DCE clock sources. This situation assumes that the PBX also takes the clocking from the central office, thereby synchronizing the clocks on the DVM and the MFT.

## cmt connect

To start the processes that perform the connection management (CMT) function and allow the ring on one fiber to be started, use the **cmt connect** command in EXEC mode.

```
cmt connect [fddi port | slot/port] [phy-a | phy-b]
```

Syntax Description		
<b>fddi</b>	(Optional)	Identifies this as a FDDI interface.
<i>port</i>	(Optional)	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>slot</i>	(Optional)	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<b>phy-a</b>	(Optional)	Selects Physical Sublayer A.
<b>phy-b</b>	(Optional)	Selects Physical Sublayer B.

## cmt disconnect

To stop the processes that perform the connection management (CMT) function and allow the ring on one fiber to be stopped, use the **cmt disconnect** command in EXEC mode.

```
cmt disconnect [fddi port | slot/port] [phy-a | phy-b]
```

Syntax Description		
<b>fddi</b>	(Optional)	Identifies this as a FDDI interface.
<i>port</i>	(Optional)	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>slot</i>	(Optional)	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<b>phy-a</b>	(Optional)	Selects Physical Sublayer A.
<b>phy-b</b>	(Optional)	Selects Physical Sublayer B.

## compress

To configure software compression for Link Access Procedure, Balanced (LAPB), PPP, and High-Level Data Link Control (HDLC) encapsulations, use the **compress** command in interface configuration mode. On Cisco 7200 series routers and Cisco 7500 series routers, hardware compression on the compression service adapter (CSA) is supported for PPP links. To disable compression, use the **no** form of this command.

```
compress {predictor | stac}
```

```
no compress {predictor | stac}
```

### Cisco VIP2 Cards

```
compress {predictor | stac [distributed | software]}
```

**Cisco 7200 Series and Cisco 7500 Series**

```
compress { predictor | stac [ csa slot | software ] }
```

**PPP Encapsulation**

```
compress [ predictor | stac | mppc [ ignore-pfc ] ]
```

Syntax Description	
<b>predictor</b>	Specifies that a predictor (RAND) compression algorithm will be used on LAPB and PPP encapsulation. Compression is implemented in the software installed in the router's main processor.
<b>stac</b>	<p>Specifies that a Stacker (LZS) compression algorithm will be used on LAPB, HDLC, and PPP encapsulation. For all platforms except Cisco 7200 series and platforms that support the VIP2, compression is implemented in the software installed in the router's main processor.</p> <p>On Cisco 7200 series, and on VIP2s in Cisco 7500 series, specifying the <b>compress stac</b> command with no options causes the router to use the fastest available compression method for PPP encapsulation only:</p> <ul style="list-style-type: none"> <li>• If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression).</li> <li>• If the CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression).</li> <li>• If the VIP2 is not available, compression is performed in the router's main processor (software compression).</li> </ul>
<b>distributed</b>	(Optional) Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the router's main processor (software compression).
<b>software</b>	(Optional) Specifies that compression is implemented in the Cisco IOS software installed in the router's main processor.
<b>csa slot</b>	(Optional) Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.
<b>mppc</b>	(Optional) Specifies that the MPPC compression algorithm will be used.
<b>ignore-pfc</b>	(Optional) Specifies that the protocol field compression flag negotiated through LCP will be ignored.

## compress mppc

To configure compression using the Microsoft PPC (MPPC) compression algorithm on your data compression Advanced Interface Module (AIM) for the Cisco 2600 series router, use the **compress mppc** command in interface configuration mode. The MPPC compression algorithm is used to exchange compressed information with a Microsoft NT remote access server. To disable compression, use the **no** form of this command.

**compress mppc**

**no compress**

---

**Syntax Description** This command has no keywords or arguments.

## compress predictor

The **compress predictor** command is replaced by the **compress** command. See the description of the **compress** command in this chapter for more information.

## compress stac caim

To specify the exact hardware compression resource preferred, enter the **compress stac caim** command in interface configuration mode. To disable compression, use the **no** form of this command.

**compress stac caim** *element-number*

**no compress stac caim** *element-number*

---

**Syntax Description**

<i>element-number</i>	Enables compression for this interface. AIM interfaces begin with 0.
-----------------------	--

## controller t1

To configure a T1 controller, use the **controller t1** command in global configuration mode. To delete the defined controller, use the **no** form of this command.

**controller t1** *dial-shelf/slot/t3-port:t1-num*

**no controller t1** *dial-shelf/slot/t3-port:t1-num*

---

**Syntax Description**

<i>dial-shelf</i>	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
<i>slot</i>	Location of the CT3 interface card in the dial shelf chassis.
<i>t3-port</i>	T3 port number. The only valid value is 0.
<i>:t1-num</i>	T1 timeslot in the T3 line. The value can be from 1 to 28.

## controller t3

To configure the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers or the CT3 feature board in Cisco AS5800 access servers, use the **controller t3** command in global configuration mode. To delete the defined controller, use the **no** form of this command.

### Cisco 7500 Series

**controller t3** *slot/port-adapter/port*

**no controller t3** *slot/port-adapter/port*

### Cisco AS5800 Access Server

**controller t3** *dial-shelf/slot/t3-port*

**no controller t3** *dial-shelf/slot/t3-port*

### Syntax Description

<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
<i>dial-shelf</i>	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
<i>slot</i>	Location of the CT3 interface card in the dial shelf chassis.
<i>t3-port</i>	T3 port number. The only valid value is 0.

## copy flash lex

To download an executable image from Flash memory on the core router to a LAN Extender, use the **copy flash lex** command in privileged EXEC mode.

**copy flash lex** *number*

### Syntax Description

<i>number</i>	Number of the LAN Extender interface to which to download an image from Flash memory.
---------------	---

## copy tftp lex

To download an executable image from a TFTP server to the LAN Extender, use the **copy tftp lex** command privileged EXEC mode.

**copy tftp lex** *number*

---

### Syntax Description

<i>number</i>	Number of the LAN Extender interface to which to download an image.
---------------	---

---

## crc

To set the length of the cyclic redundancy check (CRC) on a Fast Serial Interface Processor (FSIP) or HSSI Interface Processor (HIP) of the Cisco 7500 series routers or on a 4-port serial adapter of the Cisco 7200 series routers, use the **crc** command in interface configuration mode. To set the CRC length to 16 bits, use the **no** form of this command.

**crc** *size*

**no crc**

---

### Syntax Description

<i>size</i>	CRC size (16 or 32 bits). The default is 16 bits.
-------------	---

---

## crc4

To enable generation of CRC4 (per ITU Recommendation G.704 and G.703) to improve data integrity, use the **crc4** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**crc4**

**no crc4**

---

### Syntax Description

This command has no arguments or keywords.

## crc bits 5

To enable generation of CRC5 (per ITU Recommendation G.704 and G.703) to improve data integrity, use the **crc bits 5** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**crc bits 5**

**no crc bits 5**

**Syntax Description** This command has no arguments or keywords.

## cut-through

To configure the interfaces on the PA-12E/2FE port adapter to use cut-through switching technology between interfaces within the same bridge group, use the **cut-through** command in interface configuration mode. To return each interface to store-and-forward switching, use the **no** form of this command.

**cut-through [receive | transmit]**

**no cut-through**

<b>Syntax Description</b>	<b>receive</b>	(Optional) Selects cut-through switching technology on received data.
	<b>transmit</b>	(Optional) Selects cut-through switching technology on transmitted data.

## dce-terminal-timing enable

To prevent phase shifting of the data with respect to the clock when running the line at high speeds and long distances, use the **dce-terminal-timing enable** command in interface configuration mode. If serial clock transmit external (SCTE) terminal timing is not available from the DTE, use the **no** form of this command; the DCE will use its own clock instead of SCTE from the DTE.

**dce-terminal-timing enable**

**no dce-terminal-timing enable**

**Syntax Description** This command has no arguments or keywords.

## delay (interface)

To set a delay value for an interface, use the **delay** command in interface configuration mode. To restore the default delay value, use the **no** form of this command.

**delay** *tens-of-microseconds*

**no delay**

---

<b>Syntax Description</b>	<i>tens-of-microseconds</i>	Integer that specifies the delay in tens of microseconds for an interface or network segment. To see the default delay, use the <b>show interfaces</b> command.
---------------------------	-----------------------------	---

---

## description (controller)

To add a description to an E1 or T1 controller or the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **description** command in controller configuration mode. To remove the description, use the **no** form of this command.

**description** *string*

**no description**

---

<b>Syntax Description</b>	<i>string</i>	Comment or a description (up to 80 characters) to help you remember what is attached to an interface.
---------------------------	---------------	---

---

## down-when-looped

To configure an interface to inform the system that it is down when loopback is detected, use the **down-when-looped** command in interface configuration mode.

**down-when-looped**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## dsu bandwidth

To specify the maximum allowable bandwidth used by the PA-E3 and PA-T3 port adapters, use the **dsu bandwidth** command in interface configuration mode. To return to the default bandwidth, use the **no** form of this command.

**dsu bandwidth** *kbps*

**no dsu bandwidth**

<b>Syntax Description</b>	<i>kbps</i>	Maximum bandwidth in the range of 22 kbps to 44736 kbps. The default values are: <ul style="list-style-type: none"> <li>• 34010 kbps for PA-E3</li> <li>• 44736 kbps for PA-T3</li> </ul>
---------------------------	-------------	---

## dsu mode

To specify the interoperability mode used by a PA-E3 or PA-T3 port adapters, use the **dsu mode** command in interface configuration mode. The **dsu mode** command enables and improves interoperability with other DSUs. To return to the default mode, use the **no** form of this command.

**dsu mode** {**0** | **1** | **2**}

**no dsu mode**

<b>Syntax Description</b>	<b>0</b>	Sets the interoperability mode to 0. This is the default. Specify mode 0 to connect a PA-E3 port adapter to another PA-E3 port adapter or to a Digital Link DSU (DL3100). Use mode 0 to connect a PA-T3 port adapter to another PA-T3 port adapter or to a Digital Link DSU (DL3100).
	<b>1</b>	Sets the interoperability mode to 1. Specify mode 1 to connect a PA-E3 or PA-T3 port adapter to a Kentrox DSU.
	<b>2</b>	Sets the interoperability mode to 2. Specify mode 2 to connect a PA-T3 port adapter to a Larscom DSU.

## dte-invert-txc

On the Cisco 4000 series, you can specify the serial Network Processor Module timing signal configuration. When the board is operating as a DTE, use the **dte-invert-txc** command in interface configuration mode to invert the TXC clock signal received from the DCE. If the DCE accepts serial clock transmit external (SCTE) from the DTE, use the **no** form of this command.

**dte-invert-txc**

**no dte-invert-txc**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## duplex

To configure duplex operation on an interface, use the **duplex** command in interface configuration mode. To return the system to half-duplex mode, the system default, use the **no** form of this command.

**duplex {full | half | auto}**

**no duplex**

Syntax Description	full	half	auto
	Specifies full-duplex operation.	Specifies half-duplex operation. This is the default.	Specifies the autonegotiation capability. The interface automatically operates at half or full duplex, depending on environmental factors, such as the type of media and the transmission speeds for the peer routers, hubs, and switches used in the network configuration.

## e2-clockrate

To configure the serial interface 0 for E2 (8 MHZ full duplex) and to shut down the other three serial interfaces (1 to 3), use the **e2-clockrate** command in interface configuration mode. To disable the full duplex E2, use the **no** form of this command.

**e2-clockrate**

**no e2-clockrate**

**Syntax Description** This command has no arguments or keywords.

## early-token-release

To enable early token release on Token Ring interfaces, use the **early-token-release** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**early-token-release**

**no early-token-release**

**Syntax Description** This command has no arguments or keywords.

## encapsulation

To set the encapsulation method used by the interface, use the **encapsulation** command in interface configuration mode. To remove the encapsulation use the **no** form of this command.

**encapsulation** *encapsulation-type*

**no encapsulation** *encapsulation-type*

<b>Syntax Description</b>	<p><i>encapsulation-type</i></p> <p>Encapsulation type; one of the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>atm-dxi</b>—ATM Mode-Data Exchange Interface.</li> <li>• <b>bstun</b>—Block Serial Tunnel.</li> <li>• <b>frame-relay</b>—Frame Relay (for serial interface).</li> <li>• <b>hdlc</b>—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.</li> <li>• <b>isl</b>—Inter-Switch Link (ISL) (for virtual LANs).</li> <li>• <b>lapb</b>—X.25 Link Access Procedure, Balanced. Data link layer protocol (LAPB) DTE operation (for serial interface).</li> <li>• <b>ppp</b>—PPP (for serial interface).</li> <li>• <b>sdlc</b>—IBM serial Systems Network Architecture (SNA).</li> <li>• <b>sdlc-primary</b>—IBM serial SNA (for primary serial interface).</li> <li>• <b>sdlc-secondary</b>—IBM serial SNA (for secondary serial interface).</li> <li>• <b>slip</b>—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.</li> <li>• <b>smds</b>—Switched Multimegabit Data Services (SMDS) (for serial interface).</li> </ul>
---------------------------	--

## fdi burst-count

To allow the FCI card to preallocate buffers to handle bursty FDDI traffic (for example, Network File System (NFS) bursty traffic), use the **fdi burst-count** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

**fdi burst-count** *number*

**no fdi burst-count**

<b>Syntax Description</b>	<p><i>number</i></p> <p>Number of preallocated buffers in the range from 1 to 10. The default is 3.</p>
---------------------------	---

## fddi c-min

To set the C-Min timer on the pulse code modulation (PCM), use the **fddi c-min** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

**fddi c-min** *microseconds*

**no fddi c-min**

<b>Syntax Description</b>	<i>microseconds</i> Sets the timer value, in microseconds. The default is 1600 microseconds.
---------------------------	--

## fddi cmt-signal-bits

To control the information transmitted during the connection management (CMT) signaling phase, use the **fddi cmt-signal-bits** command in interface configuration mode.

**fddi cmt-signal-bits** *signal-bits* [**phy-a** | **phy-b**]

<b>Syntax Description</b>	<i>signal-bits</i>	A hexadecimal number preceded by 0x; for example, 0x208. The FDDI standard defines 10 bits of signaling information that must be transmitted, as follows: <ul style="list-style-type: none"> <li>bit 0—Escape bit. Reserved for future assignment by the FDDI standards committee.</li> <li>bits 1 and 2—Physical type, as defined in Table 35.</li> <li>bit 3—Physical compatibility. Set if topology rules include the connection of a physical-to-physical type at the end of the connection.</li> <li>bits 4 and 5—Link confidence test duration; set as defined in Table 36.</li> <li>bit 6—MAC available for link confidence test.</li> <li>bit 7—Link confidence test failed. The setting of bit 7 indicates that the link confidence was failed by the Cisco end of the connection.</li> <li>bit 8—MAC for local loop.</li> <li>bit 9—MAC on physical output.</li> </ul>
	<b>phy-a</b>	(Optional) Selects Physical Sublayer A. The default is 0x008 (hexadecimal) or 00 0000 1000 (binary). Bits 1 and 2 are set to 00 to select Physical A. Bit 3 is set to 1 to indicate “accept any connection.”
	<b>phy-b</b>	(Optional) Selects Physical Sublayer B. The default is 0x20c (hexadecimal) or 10 0000 1100 (binary). Bits 1 and 2 are set to 10 to select Physical B. Bit 3 is set to 1 to indicate “accept any connection.” Bit 9 is set to 1 to select MAC on output. The normal data flow on FDDI is input on Physical A and output on Physical B.

Table 35 lists the physical types.

**Table 35** FDDI Physical Type Bit Specifications

Bit 2	Bit 1	Physical Type
0	0	Physical A
1	0	Physical B
0	1	Physical S
1	1	Physical M

Table 36 lists the duration bits.

**Table 36** FDDI Link Confidence Test Duration Bit Specification

Bit 5	Bit 4	Test Duration
0	0	Short test (default 50 milliseconds)
1	0	Medium test (default 500 milliseconds)
0	1	Long test (default 5 seconds)
1	1	Extended test (default 50 seconds)

## fddi duplicate-address-check

To turn on the duplicate address detection capability on the FDDI, use the **fddi duplicate-address-check** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**fddi duplicate-address-check**

**no fddi duplicate-address-check**

**Syntax Description** This command has no arguments or keywords.

## fddi encapsulate

To specify encapsulating bridge mode on the CSC-C2/FCIT interface card, use the **fddi encapsulate** command in interface configuration mode. To turn off encapsulation bridging and return the FCIT interface to its translational, nonencapsulating mode, use the **no** form of this command.

**fddi encapsulate**

**no fddi encapsulate**

**Syntax Description** This command has no arguments or keywords.

## fddi frames-per-token

To specify the maximum number of frames that the FDDI interface will transmit per token capture, use the **fddi frames-per-token** command in interface configuration mode. To revert to the default values, use the **no** form of this command.

**fddi frames-per-token** *number*

**no fddi frames-per-token**

<b>Syntax Description</b>	<i>number</i>	Maximum number of frames to transmit per token capture. Valid values are from 1 to 10. The default is 3.
---------------------------	---------------	--

## fddi smt-frames

To enable the Station Management (SMT) frame processing capability on the FDDI, use the **fddi smt-frames** command in interface configuration mode. To disable this function and prevent the Cisco IOS software from generating or responding to SMT frames, use the **no** form of this command.

**fddi smt-frames**

**no fddi smt-frames**

<b>Syntax Description</b>	This command has no arguments or keywords.	
---------------------------	--	--

## fddi tb-min

To set the TB-Min timer in the physical connection management (PCM), use the **fddi tb-min** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

**fddi tb-min** *milliseconds*

**no fddi tb-min**

<b>Syntax Description</b>	<i>milliseconds</i>	Number that sets the TB-Min timer value. The range is 0 to 65,535 milliseconds. The default is 100 milliseconds.
---------------------------	---------------------	--

## fdi tl-min-time

To control the TL-Min time (the minimum time to transmit a Physical Sublayer, or PHY line state, before advancing to the next physical connection management [PCM] state, as defined by the X3T9.5 specification), use the **fdi tl-min-time** command in interface configuration mode.

**fdi tl-min-time** *microseconds*

<b>Syntax Description</b>	<i>microseconds</i>	Number that specifies the time used during the connection management (CMT) phase to ensure that signals are maintained for at least the value of TL-Min so the remote station can acquire the signal. The range is 0 to 4,294,967,295 microseconds. The default is 30 microseconds.
---------------------------	---------------------	---

## fdi t-out

To set the t-out timer in the physical connection management (PCM), use the **fdi t-out** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

**fdi t-out** *milliseconds*

**no fdi t-out**

<b>Syntax Description</b>	<i>milliseconds</i>	Number that sets the timeout timer. The range is 0 to 65,535 ms. The default is 100 ms.
---------------------------	---------------------	---

## fdi token-rotation-time

To control ring scheduling during normal operation and to detect and recover from serious ring error situations, use the **fdi token-rotation-time** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

**fdi token-rotation-time** *microseconds*

**no fdi token-rotation-time**

<b>Syntax Description</b>	<i>microseconds</i>	Number that specifies the token rotation time (TRT). The range is 4000 to 165,000 microseconds. The default is 5000 microseconds.
---------------------------	---------------------	---

## fddi valid-transmission-time

To recover from a transient ring error, use the **fddi valid-transmission-time** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

**fddi valid-transmission-time** *microseconds*

**no fddi valid-transmission-time**

<b>Syntax Description</b>	<i>microseconds</i>	Number that specifies the transmission valid timer (TVX) interval. The range is 2500 to 2,147,483,647 microseconds. The default is 2500 microseconds.
---------------------------	---------------------	---

## fdl

To set the Facility Data Link (FDL) exchange standard for CSU controllers or to set the FDL exchange standard for a T1 interface that uses Extended Super Frame (ESF) framing format, use the **fdl** command in controller configuration mode or ATM interface configuration mode. To disable FDL support or to specify that there is no ESF FDL, use the **no** form of this command.

### Cisco MC3810 Multiservice Access Concentrator

**fdl** {att | ansi | both}

**no fdl** {att | ansi | both}

### Cisco 2600 or 3600 Series Routers

**fdl** {att | ansi | all | none}

**no fdl** {att | ansi | all | none}

<b>Syntax Description</b>	<b>att</b>	Selects AT&T technical reference 54016 for ESF FDL exchange support.
	<b>ansi</b>	Selects ANSI T1.403 for ESF FDL exchange support.
	<b>both</b>	Specifies support for both AT&T technical reference 54016 and ANSI T1.403 for ESF FDL exchange support.
	<b>all</b>	Specifies support for both AT&T technical reference 54016 and ANSI T1.403 for ESF FDL exchange support.
	<b>none</b>	Specifies that there is no support for ESF FDL exchange.

## frame-relay

To configure Frame Relay payload compression for each Frame Relay port, use the **frame-relay** command in interface configuration mode. To terminate this form of payload compression over Frame Relay, use the **no** form of this command.

```
frame-relay payload-compression frf9 stac caim [element-number]
```

```
no frame-relay payload-compression
```

Syntax Description	
<b>payload-compression</b>	Packet-by-packet payload compression, using the Stacker method.
<b>frf9 stac</b>	Enables FRF.9 compression using the Stacker method.  If the router contains a data compression Advanced Interface Module (AIM) for the Cisco 2600 series router, compression is performed in the hardware (hardware compression).  If the compression Advanced Interface Module (CAIM) is not available, compression is performed in the software installed on the main processor of the router (software compression).
<b>caim</b> <i>element-number</i>	Enable the data compression AIM hardware compression daughtercard to do compression, at the element numbered beginning with 0 and incrementing to include all possible elements.

## frame-relay map

To enable Frame Relay compression on a data-link connection (DLC) basis, and to define mapping between a destination protocol address and the data-link connection identifier (DLCI) used to connect to the destination address, use the **frame-relay map** command in interface configuration mode. To deactivate Frame Relay compression, use the **no** form of this command.

```
frame-relay map {protocol protocol-address dlc} payload-compression frf9 stac caim  
[element-number]
```

```
no frame-relay map
```

Syntax Description	
<i>protocol</i>	Supported protocol, bridging, or logical link control keywords: <b>appletalk</b> , <b>decnet</b> , <b>dls</b> , <b>ip</b> , <b>ipx</b> , <b>llc2</b> , <b>rsrb</b> , <b>vines</b> , and <b>xns</b> .
<i>protocol-address</i>	Destination protocol address.
<b>dlci</b>	Indicates the DLCI number used to connect to the specified protocol address on the interface.
<b>payload-compression</b>	Packet-by-packet payload compression, using the Stacker method.
<b>frf9</b>	Data compression over Frame Relay.
<b>stac</b>	Specifies that a Stacker (LZS) compression algorithm will be used on LAPB, HDLC, and PPP encapsulation. Compression is implemented in the hardware Advanced Interface Module (AIM) installed in the router.

<b>caim</b>	Compression Advanced Interface Module (CAIM). Enables the data compression AIM hardware compression daughtercard to do compression.
<i>element-number</i>	(Optional) Compression element number, beginning with 0 and including all possible elements.

## framing

To select the frame type for the T1 or E1 data line, use the **framing** command in controller configuration mode.

### Syntax for T1 Lines

```
framing {sfadm | esfadm}
```

### Syntax for E1 Lines

```
framing {crc4adm | pcm30adm | clear e1}
```

### Syntax Description

<b>sfadm</b>	Specifies Super Frame as the T1 channel.
<b>esfadm</b>	Specifies Extended Super Frame as the T1 channel.
<b>crc4adm</b>	Specifies CRC4 frame as the E1 channel.
<b>pcm30adm</b>	Specifies CRC4 disabled framing mode as the E1 channel.
<b>clear e1</b>	Specifies clear-e1 framing mode for the E1 channel.

## framing (E1/T1 controller)

To select the frame type for the E1 or T1 data line, use the **framing** command in controller configuration mode.

### T1 Lines

```
framing {sf | esf}
```

### E1 Lines

```
framing {crc4 | no-crc4} [australia]
```

### Syntax Description

<b>sf</b>	Specifies Super Frame as the T1 frame type. This is the default.
<b>esf</b>	Specifies extended Super Frame as the T1 frame type.
<b>crc4</b>	Specifies CRC4 frame as the E1 frame type. This is the default for Australia.
<b>no-crc4</b>	Specifies no CRC4 frame as the E1 frame type.
<b>australia</b>	(Optional) Specifies the E1 frame type used in Australia.

## framing (E3/T3 interface)

To specify E3 or T3 line framing for a PA-E3 or PA-T3 port adapter, use the **framing** command in interface configuration mode. To return to the default G.751 framing or C-bit framing, use the **no** form of this command.

### PA-E3

**framing** {bypass | g751}

**no framing**

### PA-T3

**framing** {c-bit | m13 | bypass}

**no framing**

Syntax Description		
	<b>bypass</b>	Specifies bypass E3 framing.
	<b>g751</b>	Specifies G.751 E3 framing. This is the default for the PA-E3.
	<b>c-bit</b>	Specifies that C-bit framing is used as the T3 framing type. This is the default for the PA-T3.
	<b>m13</b>	Specifies m13 T3 framing.

## framing (T3 controller)

To specify T3 line framing used by the CT3 feature board in a Cisco AS5800 universal access server, or by the CT3IP port adapter in Cisco 7500 series routers, use the **framing** command in controller configuration mode. To restore the default framing type, use the **no** form of this command.

### Cisco AS5800 Universal Access Server

**framing** {c-bit | m23}

**no framing**

### Cisco 7500 Series Routers

**framing** {c-bit | m23 | auto-detect}

**no framing**

Syntax Description		
	<b>c-bit</b>	Specifies that C-bit framing is used as the T3 framing type. This is the default for the CT3 in a Cisco AS5800.
	<b>m23</b>	Specifies that M23 framing is used as the T3 framing type.
	<b>auto-detect</b>	Specifies that the CT3IP detects the framing type it receives from the far-end equipment. This is the default for the CT3IP in a Cisco 7500 series router.

## full-duplex

To specify full-duplex mode on full-duplex single-mode and multimode port adapters, use the **full-duplex** command in interface configuration mode. To restore the default half-duplex mode, use the **no** form of this command.

**full-duplex**

**no full-duplex**

---

**Syntax Description** This command has no arguments or keywords.

## half-duplex

To specify half-duplex mode on an Synchronous Data Link Control (SDLC) interface or on the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers, use the **half-duplex** command in interface configuration mode. To reset the interface to full-duplex mode, use the **no** form of this command.

**half-duplex**

**no half-duplex**

---

**Syntax Description** This command has no arguments or keywords.

## half-duplex controlled-carrier

To place a low-speed serial interface in controlled-carrier mode, instead of constant-carrier mode, use the **half-duplex controlled-carrier** command in interface configuration mode. To return the interface to constant-carrier mode, use the **no** form of this command.

**half-duplex controlled-carrier**

**no half-duplex controlled-carrier**

---

**Syntax Description** This command has no arguments or keywords.

## half-duplex timer

To tune half-duplex timers, use the **half-duplex timer** command in interface configuration mode. To return to the default value for that parameter, use the **no** form of this command along with the appropriate keyword.

**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* }

**no 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* }

Syntax Description	
<b>cts-delay</b> <i>value</i>	Specifies the delay introduced by the DCE interface between the time it detects the Request to Send (RTS) to the time it asserts Clear to Send (CTS) in response. The range is dependent on the serial interface hardware. The default <b>cts-delay</b> value is 0 ms.
<b>cts-drop-timeout</b> <i>value</i>	Determines the amount of time a DTE interface waits for CTS to be deasserted after it has deasserted RTS. If CTS is not deasserted during this time, an error counter is incremented to note this event. The range is 0 to 1,140,000 ms (1140 seconds). The default <b>cts-drop-timeout</b> value is 250 ms.
<b>dcd-drop-delay</b> <i>value</i>	Applies to DCE half-duplex interfaces operating in controlled-carrier mode (see the <b>half-duplex controlled-carrier</b> command). This timer determines the delay between the end of transmission by the DCE and the deassertion of Data Carrier Detect (DCD). The range is 0 to 4400 ms (4.4 seconds). The default <b>dcd-drop-delay</b> value is 100 ms.
<b>dcd-txstart-delay</b> <i>value</i>	Applies to DCE half-duplex interfaces operating in controlled-carrier mode. This timer determines the time delay between the assertion of DCD and the start of data transmission by the DCE interface. The range is 0 to 1,140,000 ms (1140 seconds). The default <b>dcd-txstart-delay</b> value is 100 ms.
<b>rts-drop-delay</b> <i>value</i>	Specifies the time delay between the end of transmission by the DTE interface and deassertion of RTS. The range is 0 to 1,140,000 ms (1140 seconds). The default <b>rts-drop-delay</b> value is 3 ms.
<b>rts-timeout</b> <i>value</i>	Determines the number of milliseconds the DTE waits for CTS to be asserted after the assertion of RTS before giving up on its transmission attempt. If CTS is not asserted in the specified amount of time, an error counter is incremented. The range is dependent on the serial interface hardware. The default <b>rts-timeout</b> value is 3 ms.
<b>transmit-delay</b> <i>value</i>	Specifies the number of milliseconds a half-duplex interface will delay the start of transmission. In the case of a DTE interface, this delay specifies how long the interface waits after something shows up in the transmit queue before asserting RTS. For a DCE interface, this dictates how long the interface waits after data is placed in the transmit queue before starting transmission. If the DCE interface is in controlled-carrier mode, this delay shows up as a delayed assertion of DCD.  This timer enables the transmitter to be adjusted if the receiver is a little slow and is not able to keep up with the transmitter. The range is 0 to 4400 ms (4.4 seconds). The default <b>transmit-delay</b> value is 0 ms.

## hold-queue

To limit the size of the IP output queue on an interface, use the **hold-queue** command in interface configuration mode. To restore the default values for an interface, use the **no** form of this command with the appropriate keyword.

**hold-queue** *length* {**in** | **out**}

**no hold-queue** {**in** | **out**}

Syntax Description		
	<i>length</i>	Integer that specifies the maximum number of packets in the queue. The range of allowed values is 0 to 65,535.
	<b>in</b>	Specifies the input queue. The default is 75 packets. For asynchronous interfaces, the default is 10 packets.
	<b>out</b>	Specifies the output queue. The default is 40 packets. For asynchronous interfaces, the default is 10 packets.

## hssi external-loop-request

To allow the router to support a CSU/DSU that uses the LC signal to request a loopback from the router, use the **hssi external-loop-request** command in interface configuration mode. To disable the feature, use the **no** form of this command.

**hssi external-loop-request**

**no hssi external-loop-request**

**Syntax Description** This command has no arguments or keywords.

## hssi internal-clock

To convert the High Speed Serial Interface (HSSI) into a clock master, use the **hssi internal-clock** command in interface configuration mode. To disable the clock master mode, use the **no** form of this command.

**hssi internal-clock**

**no hssi internal-clock**

**Syntax Description** This command has no arguments or keywords.

## hub

To enable and configure a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **hub** command in global configuration mode.

```
hub ethernet number port [end-port]
```

Syntax Description	Parameter	Description
	<b>ethernet</b>	Indicates that the hub is in front of an Ethernet interface.
	<i>number</i>	Hub number, starting with 0. Because there is only one hub, this number is 0.
	<i>port</i>	Port number on the hub. On the Cisco 2505 router, port numbers range from 1 to 8. On the Cisco 2507 router, port numbers range from 1 to 16. If a second port number follows, then the first port number indicates the beginning of a port range.
	<i>end-port</i>	(Optional) Last port number of a range.

## ignore-dcd

To configure the serial interface to monitor the DSR signal instead of the Data Carrier Detect (DCD) signal as the line up/down indicator, use the **ignore-dcd** command in interface configuration mode. To restore the default, use the **no** form of this command.

```
ignore-dcd
```

```
no ignore-dcd
```

**Syntax Description** This command has no arguments or keywords.

## ignore-hw local-loopback

To disable the monitoring of the LL pin when in DCE mode, use the **ignore-hw local-loopback** command in interface configuration mode. To return to the default, use the **no** form of this command.

```
ignore-hw local-loopback
```

```
no ignore-hw local-loopback
```

**Syntax Description** This command has no arguments or keywords.

# interface

To configure an interface type and enter interface configuration mode, use the **interface** command in global configuration mode.

```
interface type number [name-tag]
```

## Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor

```
interface type slot/port
```

## Cisco 7500 Series with Channelized T1 or E1

```
interface serial slot/port:channel-group
```

## Cisco 7500 Series with Ports on VIP Cards

```
interface type slot/port-adapter/port [ethernet | serial]
```

## Cisco 4000 Series with Channelized T1 or E1 and the Cisco MC3810

```
interface serial number:channel-group
```

To configure a subinterface, use this form of the **interface** global configuration command:

## Cisco 7200 Series

```
interface type slot/port.subinterface-number [multipoint | point-to-point]
```

## Cisco 7500 Series

```
interface type slot/port-adapter.subinterface-number [multipoint | point-to-point]
```

## Cisco 7500 Series with Ports on VIP Cards

```
interface type slot/port-adapter/port.subinterface-number [multipoint | point-to-point]
```

### Syntax Description

<i>type</i>	Type of interface to be configured. See Table 37.
<i>number</i>	Port, connector, or interface card number. On a Cisco 4000 series router, specifies the NPM number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the <b>show interfaces</b> command.
<i>name-tag</i>	(Optional) Specifies the logic name to identify the server configuration so that multiple entries of server configuration can be entered.  This optional argument is for use with the RLM feature.
<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.

<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
<b>ethernet</b>	(Optional) Ethernet IEEE 802.3 interface.
<b>serial</b>	(Optional) Serial interface.
<i>:channel-group</i>	Cisco 4000 series routers specify the T1 channel group number in the range of 0 to 23 defined with the <b>channel-group</b> controller configuration command. On a dual port card, it is possible to run channelized on one port and primary rate on the other port.  Cisco MC3810 specifies the T1/E1 channel group number in the range of 0 to 23 defined with the <b>channel-group</b> controller configuration command.
<i>.subinterface-number</i>	Subinterface number in the range 1 to 4,294,967,293. The number that precedes the period (.) must match the number to which this subinterface belongs.
<b>multipoint   point-to-point</b>	(Optional) Specifies a multipoint or point-to-point subinterface. There is no default.

Table 37 interface Type Keywords

Keyword	Interface Type
<b>async</b>	Port line used as an asynchronous interface.
<b>atm</b>	ATM interface.
<b>bri</b>	ISDN BRI. This interface configuration is propagated to each of the B channels. B channels cannot be individually configured. The interface must be configured with dial-on-demand commands in order for calls to be placed on that interface.
<b>dialer</b>	Dialer interface.
<b>ethernet</b>	Ethernet IEEE 802.3 interface.
<b>fastethernet</b>	100-Mbps Ethernet interface on the Cisco 4500, Cisco 4700, Cisco 7000, and Cisco 7500 series routers.
<b>fddi</b>	FDDI.
<b>group-async</b>	Master asynchronous interface.
<b>hssi</b>	High-Speed Serial Interface (HSSI).
<b>lex</b>	LAN Extender (LEX) interface.
<b>loopback</b>	Software-only loopback interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The <i>interface-number</i> is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.
<b>null</b>	Null interface.
<b>port-channel</b>	Port channel interface
<b>pos</b>	Packet OC-3 interface on the Packet over SONET Interface Processor.
<b>serial</b>	Serial interface.
<b>switch</b>	Switch interface

Table 37 *interface Type Keywords (continued)*

Keyword	Interface Type
<b>tokenring</b>	Token Ring interface.
<b>tunnel</b>	Tunnel interface; a virtual interface. The <i>number</i> is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
<b>vg-anylan</b>	100VG-AnyLAN port adapter.

## interface ctunnel

To create a virtual interface to transport IP over a Connectionless Network Service (CLNS) tunnel (CTunnel), use the **interface ctunnel** command in global configuration mode. To remove the virtual interface, use the **no** form of this command.

**interface ctunnel** *interface-number*

**no interface ctunnel** *interface-number*

### Syntax Description

<i>interface-number</i>	CTunnel interface number (a number from 0 through 2,147,483,647).
-------------------------	---



## Interface Commands: interface fastethernet Through service-module t1 remote-loopback

This chapter describes the function and syntax of the interface commands: **interface fastethernet** through **service-module t1 remote-loopback**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Interface Command Reference*.

### interface fastethernet

To select a particular Fast Ethernet interface for configuration, use the **interface fastethernet** command in global configuration mode.

#### Cisco 4500 and 4700 Series

```
interface fastethernet number
```

#### Cisco 7200 Series

```
interface fastethernet slot/port
```

#### Cisco 7500 Series

```
interface fastethernet slot/port-adapter/port
```

Syntax Description		
	<i>number</i>	Port, connector, or interface card number. On a Cisco 4500 or 4700 series routers, specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
	<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## interface gigabitethernet

To configure a Gigabit Ethernet interface and enter interface configuration mode, use the **interface gigabitethernet slot/port** command in global configuration mode.

```
interface gigabitethernet slot/port
```

To configure a Gigabit Ethernet interface and enter interface configuration mode on a Cisco 7200 VXR router used as a router shelf in an AS5800 Universal Access Server, use the **interface gigabitethernet router-shelf/slot/port** command in global configuration mode.

```
interface gigabitethernet router-shelf/slot/port
```

Syntax Description		
	<i>router-shelf</i>	Router shelf in a Cisco AS5800 Universal Access Server.
	<i>slot</i>	Slot number of the interface.
	<i>port</i>	Port number on the interface.

## interface group-async

To create a group interface that will serve as master to which asynchronous interfaces can be associated as members, use the **interface group-async** command in global configuration mode. To restore the default, use the **no** form of this command.

```
interface group-async unit-number
```

```
no interface group-async unit-number
```

Syntax Description		
	<i>unit-number</i>	Number of the asynchronous group interface being created.

## interface port-channel

To specify a Fast EtherChannel and enter interface configuration mode, use the **interface port-channel** command in global configuration mode.

```
interface port-channel channel-number
```

Syntax Description		
	<i>channel-number</i>	Channel number assigned to this port-channel interface. Range is 1 to 4.

## interface pos

To specify the Packet OC-3 interface on the Packet-over-SONET (POS) interface processor and enter interface configuration mode, use the **interface pos** command in global configuration mode.

### Cisco 7000 and Cisco 7500 Series Routers with VIPs

```
interface pos slot/port-adapter/port
```

### Cisco 7200 Series Routers

```
interface pos slot/port
```

Syntax Description	slot	Specifies the backplane slot number.
	port	On Cisco 7000 series and Cisco 7500 series routers, specifies the ports on a VIP card. The value must be 0.
	port-adapter	Port adapter number on the interface. The value must be 0.

## interface vg-anylan

To specify the interface on a 100VG-AnyLAN port adapter and enter interface configuration mode on Cisco 7200 series routers and Cisco 7500 series routers, use the **interface vg-anylan** command in global configuration mode.

### Cisco 7200 Series Routers

```
interface vg-anylan slot/port
```

### Cisco 7500 Series Routers with VIPs

```
interface vg-anylan slot/port-adapter/port
```

Syntax Description	slot	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	port	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	port-adapter	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## international bit

To set the E3 international bit in the G.751 frame used by the PA-E3 port adapter, use the **international bit** command in interface configuration mode. To return to the default international bit, use the **no** form of this command.

**international bit** {0 | 1} {0 | 1}

**no international bit**

<b>Syntax Description</b>	<b>0   1</b>	Specifies the value of the first international bit in the G.751 frame. The default is 0.
	<b>0   1</b>	Specifies the value of the second international bit in the G.751 frame. The default is 0.

## invert data

To invert the data stream, use the **invert data** command in interface configuration mode. This command applies only to the Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7200 series routers, and Cisco 7500 series routers. To disable inverting the data stream, use the **no** form of this command.

**invert data**

**no invert data**

**Syntax Description** This command has no arguments or keywords.

## invert rxclock

To configure UIO serial port 0 or 1 on the Cisco MC3810 when the cable connected is DCE type, use the **invert rxclock** command in interface configuration mode. The command inverts the phase of the RX clock on the UIO serial interface, which does not use the T1/E1 interface. To disable the phase inversion, use the **no** form of this command.

**invert rxclock**

**no invert rxclock**

**Syntax Description** This command has no arguments or keywords.

## invert-transmit-clock

The **invert-transmit-clock** command is replaced by the **invert txclock** command. See the description of the **invert-txclock** command in this chapter for information on the transmit clock signal.

## invert txclock

To invert the transmit clock signal, use the **invert txclock** command in interface configuration mode. This command applies only to Cisco 7200 series and Cisco 7500 series routers. To return the transmit clock signal to its initial state, use the **no** form of this command.

**invert txclock**

**no invert txclock**

---

**Syntax Description** This command has no arguments or keywords.

## ip director default-weights

To configure default weight metrics for the DistributedDirector, use the **ip director default-weights** command in global configuration mode. To restore the default, use the **no** form of this command.

**ip director default-weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*] }

**no ip director default-weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*] }

---

<b>Syntax Description</b>	<b>drp-int</b> <i>n</i>	<p>(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (<b>drp-ext</b>) to help determine the distance between the router and the client originating the DNS query.</p> <p>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.</p>
	<b>drp-ext</b> <i>n</i>	<p>(Optional) DRP external metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.</p>

---

<b>drp-ser</b> <i>n</i>	(Optional) DRP server metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric ( <b>drp-int</b> ) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.  If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.
<b>drp-rtt</b> <i>n</i>	(Optional) DRP round-trip time metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
<b>random</b> <i>n</i>	(Optional) Random metric. The range is 1 to 100.  This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
<b>admin</b> <i>n</i>	(Optional) Administrative metric. The range is 1 to 100.  This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
<b>portion</b> <i>n</i>	(Optional) Portion metric. The range is 1 to 100.  This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
<b>availability</b> <i>n</i>	(Optional) Availability metric. The range is 1 to 65,535.  This option specifies the load information for the DistributedDirector. The default value is 65,535.
<b>route-map</b> <i>n</i>	(Optional) Route-map metric. The range is 1 to 100.  This option specifies if a server should be offered to a client.

## ip director dfp

To configure the DistributedDirector Dynamic Feedback Protocol (DFP) agent with which the DistributedDirector should communicate, use the **ip director dfp** command in global configuration mode. To turn off the DFP agent, use the **no** form of this command.

**ip director dfp** *ip-address* [*port*] [**retry** *n*] [**attempts** *n*] [**timeout** *n*]

**no ip director dfp** *ip-address* [*port*] [**retry** *n*] [**attempts** *n*] [**timeout** *n*]

Syntax Description		
	<i>ip-address</i>	IP address.
	<i>port</i>	(Optional) Port number to which the distributed servers are configured. The default value is 8080.
	<b>retry</b> <i>n</i>	(Optional) Number of times a connection will be attempted. The default value is 5 attempts.
	<b>attempts</b> <i>n</i>	(Optional) Delay, in seconds, between each attempt. The default value is 10,000 seconds.
	<b>timeout</b> <i>n</i>	(Optional) Maximum amount of time, in seconds, for which DFP information is assumed valid. The default value is 10,000 seconds.

## ip director dfp security

To configure a security key for use when connecting to the Dynamic Feedback Protocol (DFP) client named, use the **ip director dfp security** command in global configuration mode. To turn off the security key, use the **no** form of this command.

```
ip director dfp security ip-address md5 string [timeout]
```

```
no ip director dfp security ip-address md5 string [timeout]
```

Syntax Description		
	<i>ip-address</i>	IP address for the service.
	<b>md5</b>	Security data authentication. Message Digest 5.
	<i>string</i>	Security key.
	<i>timeout</i>	(Optional) Amount of time, in seconds, during which DistributedDirector will continue to accept a previously defined security key. The default value is 0 seconds.

## ip director host priority

To configure the order in which the DistributedDirector considers metrics when picking a server, use the **ip director host priority** command in global configuration mode. To turn off metric priorities, use the **no** form of this command.

```
ip director host host-name priority {[drp-int n] [drp-ext n] [drp-ser n] [drp-rtt n] [random n] [admin n] [portion n] [availability n] [route-map n] }
```

```
no ip director host host-name priority {[drp-int n] [drp-ext n] [drp-ser n] [drp-rtt n] [random n] [admin n] [portion n] [availability n] [route-map n] }
```

**Syntax Description**

<i>host-name</i>	Name of the host that maps to one or more IP addresses. Do not use an IP address.
<b>drp-int</b> <i>n</i>	<p>(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (<b>drp-ext</b>) to help determine the distance between the router and the client originating the DNS query.</p> <p>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.</p>
<b>drp-ext</b> <i>n</i>	<p>(Optional) DRP external metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.</p>
<b>drp-ser</b> <i>n</i>	<p>(Optional) DRP server metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (<b>drp-int</b>) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.</p> <p>If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.</p>
<b>drp-rtt</b> <i>n</i>	<p>(Optional) DRP round-trip time metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.</p>
<b>random</b> <i>n</i>	<p>(Optional) Random metric. The range is 1 to 100.</p> <p>This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.</p>
<b>admin</b> <i>n</i>	<p>(Optional) Administrative metric. The range is 1 to 100.</p> <p>This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.</p>

<b>portion</b> <i>n</i>	(Optional) Portion metric. The range is 1 to 100.  This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
<b>availability</b> <i>n</i>	(Optional) Availability metric. The range is 1 to 65,535.  This option specifies the load information for the DistributedDirector. The default value is 65,535.
<b>route-map</b> <i>n</i>	(Optional) Route-map metric. The range is 1 to 100.  This option specifies if a server should be offered to a client.

## ip director host weights

To set host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name, use the **ip director host weights** command in global configuration mode. To turn off weights for a host, use the **no** form of this command.

**ip director host** *host-name* **weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

**no ip director host** *host-name* **weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

### Syntax Description

<i>host-name</i>	Name of the host that maps to one or more IP addresses. Do not use an IP address.
<b>drp-int</b> <i>n</i>	(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric ( <b>drp-ext</b> ) to help determine the distance between the router and the client originating the DNS query.  If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.
<b>drp-ext</b> <i>n</i>	(Optional) DRP external metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.

<b>drp-ser</b> <i>n</i>	(Optional) DRP server metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric ( <b>drp-int</b> ) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.  If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.
<b>drp-rtt</b> <i>n</i>	(Optional) DRP round-trip time metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
<b>random</b> <i>n</i>	(Optional) Random metric. The range is 1 to 100.  This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
<b>admin</b> <i>n</i>	(Optional) Administrative metric. The range is 1 to 100.  This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
<b>portion</b> <i>n</i>	(Optional) Portion metric. The range is 1 to 100.  This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
<b>availability</b> <i>n</i>	(Optional) Availability metric. The range is 1 to 65,535.  This option specifies the load information for the DistributedDirector. The default value is 65,535.
<b>route-map</b> <i>n</i>	(Optional) Route-map metric. The range is 1 to 100.  This option specifies if a server should be offered to a client.

## ip director server availability

To configure a default availability value for all ports on a server, use the **ip director server availability** command in global configuration mode. To restore the default, use the **no** form of this command.

**ip director server** *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

**no ip director server** *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

Syntax Description		
	<i>ip-address</i>	IP address.
	<i>availability-value</i>	Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535.
	<b>dfp</b> [ <i>availability-value</i> ]	Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535.

## ip director server port availability

To configure a default availability value for a specific port on a server, use the **ip director server port availability** command in global configuration mode. To restore the default, use the **no** form of this command.

```
ip director server ip-address port availability {availability-value | dfp [availability-value]}
```

```
no ip director server ip-address port availability {availability-value | dfp [availability-value]}
```

Syntax Description		
	<i>ip-address</i>	IP address.
	<i>availability-value</i>	Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535.
	<b>dfp</b> [ <i>availability-value</i> ]	Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535.

## keepalive

To set the keepalive timer for a specific interface, use the **keepalive** command in interface configuration mode. To turn off keepalives entirely, use the **no** form of this command.

```
keepalive [seconds]
```

```
no keepalive [seconds]
```

Syntax Description		
	<i>seconds</i>	(Optional) Integer value greater than 0. The default is 10.

## lbo

To set a cable length longer than 655 feet for a DS-1 link, use the **lbo** command in interface configuration mode on the interface for a T1 link. To delete the **lbo** value, use the **no** form of this command.

```
lbo {long {gain26 | gain36} {-15db | -22.5db | -7.5db | 0db} | short {133 | 266 | 399 | 533 | 655}}
```

```
no lbo
```

Syntax Description		
	<b>gain26</b>	Specifies the decibel pulse gain at 26 decibels. This is the default pulse gain.
	<b>gain36</b>	Specifies the decibel pulse gain at 36 decibels.
	<b>-15db</b>	Specifies the decibel pulse rate at -15 decibels.
	<b>-22.5db</b>	Specifies the decibel pulse rate at -22.5 decibels.
	<b>-7.5db</b>	Specifies the decibel pulse rate at -7.5 decibels.
	<b>0db</b>	Specifies the decibel pulse rate at 0 decibels. This is the default.
	<b>133</b>	Specifies a cable length from 0 to 133 feet.
	<b>266</b>	Specifies a cable length from 133 to 266 feet.
	<b>399</b>	Specifies a cable length from 266 to 399 feet.
	<b>533</b>	Specifies a cable length from 399 to 533 feet.
	<b>655</b>	Specifies a cable length from 533 to 655 feet.

## lex burned-in-address

To set the burned-in MAC address for a LAN Extender interface, use the **lex burned-in-address** command in interface configuration mode. To clear the burned-in MAC address, use the **no** form of this command.

**lex burned-in-address** *ieee-address*

**no lex burned-in-address**

Syntax Description	<i>ieee-address</i>	48-bit IEEE MAC address written as a dotted triplet of 4-digit hexadecimal numbers.
--------------------	---------------------	---

## lex input-address-list

To assign an access list that filters on MAC addresses, use the **lex input-address-list** command in interface configuration mode. To remove an access list from the interface, use the **no** form of this command.

**lex input-address-list** *access-list-number*

**no lex input-address-list**

Syntax Description	<i>access-list-number</i>	Number of the access list assigned with the <b>access-list</b> global configuration command. It can be a number from 700 to 799.
--------------------	---------------------------	--

## lex input-type-list

To assign an access list that filters Ethernet packets by type code, use the **lex input-type-list** command in interface configuration mode. To remove an access list from an interface, use the **no** form of this command.

**lex input-type-list** *access-list-number*

**no lex input-type-list**

---

<b>Syntax Description</b>	<i>access-list-number</i>	Number of the access list that you assigned with the <b>access-list</b> command. It can be a number in the range 200 to 299.
---------------------------	---------------------------	--

---

## lex priority-group

To activate priority output queuing on the LAN Extender, use the **lex priority-group** command in interface configuration mode. To disable priority output queuing, use the **no** form of this command.

**lex priority-group** *group*

**no lex priority-group**

---

<b>Syntax Description</b>	<i>group</i>	Number of the priority group. It can be a number in the range 1 to 10.
---------------------------	--------------	--

---

## lex retry-count

To define the number of times to resend commands to the LAN Extender chassis, use the **lex retry-count** command in interface configuration mode. To return to the default value, use the **no** form of this command.

**lex retry-count** *number*

**no lex retry-count** *number*

---

<b>Syntax Description</b>	<i>number</i>	Number of times to retry sending commands to the LAN Extender. It can be a number in the range 0 to 100. The default is 10.
---------------------------	---------------	---

---

## lex timeout

To define the amount of time to wait for a response from the LAN Extender, use the **lex timeout** command in interface configuration mode. To return to the default time, use the **no** form of this command.

**lex timeout** *milliseconds*

**no lex timeout** [*milliseconds*]

### Syntax Description

<i>milliseconds</i>	Time, in milliseconds, to wait for a response from the LAN Extender before resending the command. It can be a number in the range 500 to 60,000. The default is 2000 ms.
---------------------	--

## linecode

To select the line-code type for T1 or E1 lines, use the **linecode** command in controller configuration mode.

**linecode** {**ami** | **b8zs** | **hdb3**}

### Syntax Description

<b>ami</b>	Specifies alternate mark inversion (AMI) as the line-code type. Valid for T1 or E1 controllers. This is the default for T1 lines.
<b>b8zs</b>	Specifies B8ZS as the line-code type. Valid for T1 controller only.
<b>hdb3</b>	Specifies high-density bipolar 3 (hdb3) as the line-code type. Valid for E1 controller only. This is the default for E1 lines.

## line-termination

To specify the line termination for the E1 port on a trunk card, use the **line-termination** command in controller configuration mode. To return to the default line termination, use the **no** form of this command.

**line-termination** {**75-ohm** | **120-ohm**}

**no line-termination**

### Syntax Description

<b>75-ohm</b>	Specifies 75-ohm unbalanced termination.
<b>120-ohm</b>	Specifies 120-ohm balanced termination. This is the default.

## link-test

To reenable the link-test function on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **link-test** command in hub configuration mode. Use the **no** form of this command to disable this feature if a pre-10BaseT twisted-pair device not implementing link test is connected to the hub port.

**link-test**

**no link-test**

---

**Syntax Description**

This command has no arguments or keywords.

## local-lnm

To enable Lanoptics Hub Networking Management of a PCbus Token Ring interface, use the **local-lnm** command in interface configuration mode. To disable Lanoptics Hub Networking Management, use the **no** form of this command.

**local-lnm**

**no local-lnm**

---

**Syntax Description**

This command has no arguments or keywords.

## loopback (interface)

To diagnose equipment malfunctions between the interface and device, use the **loopback** command in interface configuration mode. To disable the test, use the **no** form of this command.

**loopback**

**no loopback**

---

**Syntax Description**

This command has no arguments or keywords.

## loopback (E3/T3 interface)

To loop the serial interface on a PA-E3 or PA-T3 port adapter, use the **loopback** command in interface configuration mode. To remove the loopback, use the **no** form of this command.

### PA-E3 Port Adapter

```
loopback {dte | local | network {line | payload}}
```

```
no loopback
```

### PA-T3 Port Adapter

```
loopback {dte | local | network {line | payload} | remote}
```

```
no loopback
```

Syntax Description		
<b>dte</b>		Sets the loopback after the LIU toward the terminal.
<b>local</b>		Sets the loopback after going through the framer toward the terminal.
<b>network {line   payload}</b>		Sets the loopback toward the network before going through the framer ( <b>line</b> ) or after going through the framer ( <b>payload</b> ).
<b>remote</b>		Sends a far-end alarm control (FEAC) to set the remote framer in loopback.

## loopback (T1 interface)

To loop individual T1 channels on the CT3IP in Cisco 7000 series routers with the RSP7000 and RSP7000CI and in Cisco 7500 series routers, use the **loopback** command in interface configuration mode. To remove the loopback, use the **no** form of this command.

```
loopback [local | network {line | payload} | remote {line {fdl {ansi | bellcore} | inband} | payload [fdl] [ansi]]]
```

```
no loopback
```

Syntax Description		
<b>local</b>		(Optional) Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) signal out toward the network.
<b>network {line   payload}</b>		(Optional) Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the High-Level Data Link Control (HDLC) controllers (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers (payload).

<b>remote line fdl</b> {ansi   bellcore}	(Optional) Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (00001110 11111111 for FDL ANSI and 00010010 11111111 for FDL Bellcore) to the remote end requesting that it enter into a network line loopback. Specify the <b>ansi</b> keyword to enable the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, per the ANSI T1.403 Specification. Specify the <b>bellcore</b> keyword to enable the remote SmartJack loopback on the T1 channel, per the TR-TSY-000312 Specification.
<b>remote line inband</b>	(Optional) Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback.
<b>remote payload</b> [fdl] [ansi]	(Optional) Sends a repeating, 16-bit ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel.  You can optionally specify <b>fdl</b> and <b>ansi</b> , but it is not necessary.

## loopback (T3 controller)

To loop the entire T3 (all 28 T1 channels) on the CT3 in a Cisco AS5800 universal access server or on the CT3IP in Cisco 7500 series routers, use the **loopback** command in controller configuration mode. To remove the loopback, use the **no** form of this command.

**loopback** [local | network | remote]

**no loopback**

Syntax Description	
<b>local</b>	(Optional) Loops the data back toward the router and sends an alarm indication signal (AIS) signal out toward the network.
<b>network</b>	(Optional) Loops the data toward the network at the T1 framer.
<b>remote</b>	(Optional) 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. The type of framing used is determined by the equipment you are connecting to (for more information, see the <b>framing</b> controller command).

## loopback applique

To configure an internal loop on the High Speed Serial Interface (HSSI) applique, use the **loopback applique** command in interface configuration mode. To remove the loop, use the **no** form of this command.

**loopback applique**

**no loopback applique**

Syntax Description	
	This command has no arguments or keywords.

## loopback dte

To loop packets back to the DTE from the CSU/DSU, when the device supports this feature, use the **loopback dte** command in interface configuration mode. To remove the loop, use the **no** form of this command.

**loopback dte**

**no loopback dte**

---

**Syntax Description** This command has no arguments or keywords.

## loopback line

To loop packets completely through the CSU/DSU to configure the CSU loop, use the **loopback line** command in interface configuration mode. To remove the loop, use the **no** form of this command.

**loopback line [payload]**

**no loopback line [payload]**

---

<b>Syntax Description</b>	<b>payload</b>	(Optional) Configures a loopback point at the DSU and loops data back to the network on an integrated CSU/DSU.
---------------------------	----------------	--

---

## loopback remote (interface)

To loop packets through a CSU/DSU, over a DS-3 link or a channelized T1 link, to the remote CSU/DSU and back, use the **loopback remote** command in interface configuration mode. To remove the loopback, use the **no** form of this command.

### FT1/T1 CSU/DSU Modules

**loopback remote {full | payload | smart-jack} [0in1 | 1in1 | 1in2 | 1in5 | 1in8 | 3in24 | qrw | user-pattern *24bit-binary-value*]**

**no loopback remote {full | payload | smart-jack}**

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

**loopback remote [2047 | 511 | stress-pattern *pattern-number*]**

**no loopback remote**

**Syntax Description**

<b>full</b>	Transmits a full-bandwidth line loopback request to a remote device, which is used for testing.
<b>payload</b>	Transmits a payload line loopback request to a remote device, which is used for testing the line and remote DSU.
<b>smart-jack</b>	Transmits a loopback request to the remote smart-jack, which some service providers attach on the line before the customer premises equipment (CPE). You cannot put the local smart jack into loopback.
<b>0in1</b>	(Optional) Transmits an all-zeros test pattern used for verifying B8ZS line encoding. The remote end may report a loss of signal when using alternate mark inversion (AMI) line coding.
<b>1in1</b>	(Optional) Transmits an all-ones test pattern used for signal power measurements.
<b>1in2</b>	(Optional) Transmits an alternating ones and zeroes test pattern used for testing bridge taps.
<b>1in5</b>	(Optional) Transmits the industry standard test-pattern loopback request.
<b>1in8</b>	(Optional) Transmits a test pattern used for stressing timing recovery of repeaters.
<b>3in24</b>	(Optional) Transmits a test pattern used for testing the ones density tolerance on AMI lines.
<b>qrw</b>	(Optional) Transmits a quasi-random word test pattern, which is a random signal that simulates user data.
<b>user-pattern</b> <i>24bit-binary-value</i>	(Optional) Transmits a test pattern that you define. Enter a binary string up to 24 bits long. For the fixed patterns such 0in1 and 1in1, the T1 framing bits are jammed on top of the test pattern; for the user-pattern, the pattern is simply repeated in the time slots.
<b>2047</b>	(Optional) Transmits a pseudorandom test pattern that repeats after 2047 bits.
<b>511</b>	(Optional) Transmits a pseudorandom test pattern that repeats after 511 bits.
<b>stress-pattern</b> <i>pattern-number</i>	(Optional) Transmits a DDS stress pattern available only on the 4-wire 56/64-kbps CSU/DSU module. You may enter a stress pattern from 1 to 4. A 1 pattern sends 100 bytes of all 1s and then 100 bytes of all 0s to test the stress clocking of the network. A 2 pattern sends 100 bytes of a 0x7e pattern and then 100 bytes of all 0s. A 3 pattern sends continuous bytes of a 0x46 pattern. A 4 pattern sends continuous bytes of 0x02 pattern.

## mdl

To configure the Maintenance Data Link (MDL) message defined in the ANSI T1.107a-1990 specification for the CT3 in a Cisco AS5800 universal access server, or for the CT3IP in Cisco 7500 series routers, use the **mdl** command in interface configuration mode. To remove the message, use the **no** form of this command.

```
mdl { transmit { path | idle-signal | test-signal } | string { eic | lic | fic | unit | pfi | port | generator }
      string }
```

```
no mdl { transmit { path | idle-signal | test-signal } | string { eic | lic | fic | unit | pfi | port
      | generator } string }
```

Syntax Description		
<b>transmit path</b>		Enables transmission of the MDL Path message.
<b>transmit idle-signal</b>		Enables transmission of the MDL Idle Signal message.
<b>transmit test-signal</b>		Enables transmission of the MDL Test Signal message.
<b>string eic</b> <i>string</i>		Specifies the Equipment Identification Code; can be up to 10 characters.
<b>string lic</b> <i>string</i>		Specifies the Location Identification Code; can be up to 11 characters.
<b>string fic</b> <i>string</i>		Specifies the Frame Identification Code; can be up to 10 characters.
<b>string unit</b> <i>string</i>		Specifies the Unit Identification Code; can be up to 6 characters.
<b>string pfi</b> <i>string</i>		Specifies the Facility Identification Code sent in the MDL Path message; can be up to 38 characters.
<b>string port</b> <i>string</i>		Specifies the Port number string sent in the MDL Idle Signal message; can be up to 38 characters.
<b>string generator</b> <i>string</i>		Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters.

## media-type

To specify the physical connection on an interface, use the **media-type** command in interface configuration mode. To restore the default value, use the **no** form of this command.

```
media-type { aui | 10baset | 100baset | mii }
```

```
no media-type { aui | 10baset | 100baset | mii }
```

Syntax Description		
<b>aui</b>		Selects an AUI 15-pin physical connection. This is the default on Cisco 4000 series routers.
<b>10baset</b>		Selects an R-J45 10BASE-T physical connection.
<b>100baset</b>		Specifies an RJ-45 100BASE-T physical connection. This is the default on Cisco 7000 series and Cisco 7200 series routers.
<b>mii</b>		Specifies a media-independent interface.

## media-type half-duplex

The **media-type half-duplex** command is replaced by the **half-duplex** command. See the description of the **half-duplex** command in this chapter for more information.

## mop enabled

To enable an interface to support the Maintenance Operation Protocol (MOP), use the **mop enabled** command in interface configuration mode. To disable MOP on an interface, use the **no** form of this command.

**mop enabled**

**no mop enabled**

---

**Syntax Description** This command has no arguments or keywords.

## mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mop sysid** command in interface configuration mode. To disable MOP message support on an interface, use the **no** form of this command.

**mop sysid**

**no mop sysid**

---

**Syntax Description** This command has no arguments or keywords.

## mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

**mtu** *bytes*

**no mtu**

---

**Syntax Description**

<i>bytes</i>	Desired size in bytes.
--------------	------------------------

---

## national bit

To set the E3 national bit in the G.751 frame used by the PA-E3 port adapter, use the **national bit** command in interface configuration mode. To return to the default E3 national bit, use the **no** form of this command.

**national bit {0 | 1}**

**no national bit**

<b>Syntax Description</b>	<b>0   1</b> Specifies the E3 national bit in the G.751 frame. The default is 0.
---------------------------	--

## national reserve

To set the E1 national bit, enter the **national reserve** command in interface configuration mode. To return to the default E1 national bit, use the **no** form of this command.

**national reserve <0-1><0-1><0-1><0-1><0-1><0-1>**

**no national reserve**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## negotiation

To configure speed, duplex, and flow control on the Gigabit Ethernet port of the Cisco 7200-I/O-GE+E, use the **negotiation** command in interface configuration mode. To disable automatic negotiation, use the **no negotiation auto** command.

**negotiation {forced | auto}**

**no negotiation auto**

<b>Syntax Description</b>	<b>forced</b> Disables flow control and configures the Gigabit Ethernet interface in 1000/full-duplex mode.
	<b>auto</b> Enables the autonegotiation protocol to configures the speed, duplex, and automatic flow-control of the Gigabit Ethernet interface.

## nrzi-encoding

To enable nonreturn-to-zero inverted (NRZI) line-coding format, use the **nrzi-encoding** command in interface configuration mode. To disable this capability, use the **no** form of this command.

**nrzi-encoding [mark]**

**no nrzi-encoding**

<b>Syntax Description</b>	<b>mark</b>	(Optional) Specifies that NRZI mark encoding is required on the PA-8T and PA-4T+ synchronous serial port adapters on Cisco 7200 and 7500 series routers. If mark is not specified, NRZI space encoding is used.
---------------------------	-------------	---

## physical-layer

To specify the mode of a slow-speed serial interface on a router as either synchronous or asynchronous, use the **physical-layer** command in interface configuration mode. To return the interface to the default mode of synchronous, use the **no** form of this command.

**physical-layer {sync | async}**

**no physical-layer**

<b>Syntax Description</b>	<b>sync</b>	Places the interface in synchronous mode. This is the default.
	<b>async</b>	Places the interface in asynchronous mode.

## port

To enable an interface on a PA-4R-DTR port adapter to operate as a concentrator port, use the **port** command in interface configuration mode. To restore the default station mode, use the **no** form of this command.

**port**

**no port**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## pos ais-shut

To send the line alarm indication signal (LAIS) when the Packet-Over-SONET (POS) interface is placed in any administrative shut down state, use the **pos ais-shut** command in interface configuration mode.

```
pos ais-shut
```

**Syntax Description** This command has no keywords or arguments.

## pos flag

To set the SONET overhead bytes in the frame header to meet a specific standards requirement or to ensure interoperability with the equipment of another vendor, use the **pos flag** command in interface configuration mode. To remove the setting of the SONET overhead bytes, use the **no** form of this command.

```
pos flag {c2 | j0 | s1s0} value
```

```
no pos flag {c2 | j0 | s1s0} value
```

Syntax Description		
<b>c2</b> <i>value</i>		Path signal identifier used to identify the payload content type. The default value is 0xCF.
<b>j0</b> <i>value</i>		Section trace byte (formerly the C1 byte). For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. The byte value can be 0 to 255.
<b>s1s0</b> <i>value</i>		S1 and S0 bits (bits 5 and 6 of the H1 #1 payload pointer byte). Use the following values to tell the SONET transmission equipment the SS bit: <ul style="list-style-type: none"> <li>For OC-3c, use 0 (this is the default).</li> <li>For AU-4 container in SDH, use 2.</li> </ul> <p>The S1 and S0 bits can be 0 to 3. Values 1 and 3 are undefined. The default value is 0.</p>

## pos framing

To specify the framing used on the POS (Packet-over-SONET) interface, use the **pos framing** command in interface configuration mode. To return to the default SONET STS-3c framing mode, use the **no** form of this command.

```
pos framing {sdh | sonet}
```

```
no pos framing
```

Syntax Description		
<b>sdh</b>		Selects SDH STM-1 framing. This framing mode is typically used in Europe.
<b>sonet</b>		Selects SONET STS-3c framing. This is the default.

## pos framing-sdh

The **pos framing-sdh** command is replaced by the **pos framing** command. See the description of the **pos framing** command in this chapter for more information.

## pos internal-clock

The **pos internal-clock** command is replaced by the **clock source (interface)** command. See the description of the **clock source (interface)** command in this chapter for information on transmit clock source.

## pos report

To permit selected SONET alarms to be logged to the console for a POS (Packet-Over-SONET) interface, use the **pos report** command in interface configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

```
pos report {b1-tca | b2-tca | b3-tca | lais | lrldi | pais | plop | prdi | rdool | sd-ber | sf-ber | slof |
slos}
```

```
no pos report {b1-tca | b2-tca | b3-tca | lais | lrldi | pais | plop | prdi | rdool | sd-ber | sf-ber | slof
| slos}
```

### Syntax Description

<b>b1-tca</b>	Reports B1 bit-error rate (BER) threshold crossing alarm (TCA) errors.
<b>b2-tca</b>	Reports B2 BER crossing TCA errors.
<b>b3-tca</b>	Reports B3 BER crossing TCA errors.
<b>lais</b>	Reports line alarm indication signal errors.
<b>lrldi</b>	Reports line remote defect indication errors.
<b>pais</b>	Reports path alarm indication signal errors.
<b>plop</b>	Reports path loss of pointer errors.
<b>prdi</b>	Reports path remote defect indication errors.
<b>rdool</b>	Reports receive data out of lock errors.
<b>sd-ber</b>	Reports signal degradation BER errors.
<b>sf-ber</b>	Reports signal failure BER errors.
<b>slof</b>	Reports section loss of frame errors.
<b>slos</b>	Reports section los of signal errors.

## pos scramble-atm

To enable SONET payload scrambling on a POS (Packet-Over-SONET) interface, use the **pos scramble-atm** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

```
pos scramble-atm
```

```
no pos scramble-atm
```

**Syntax Description** This command has no arguments or keywords.

## pos threshold

To set the bit-error rate (BER) threshold values of the specified alarms for a POS (Packet-Over-SONET) interface, use the **pos threshold** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
pos threshold {b1-tca | b2-tca | b3-tca | sd-ber | sf-ber} rate
```

```
no pos threshold {b1-tca | b2-tca | b3-tca | sd-ber | sf-ber} rate
```

### Syntax Description

<b>b1-tca</b>	B1 BER threshold crossing alarm. The default is 6.
<b>b2-tca</b>	B2 BER threshold crossing alarm. The default is 6.
<b>b3-tca</b>	B3 BER threshold crossing alarm. The default is 6.
<b>sd-ber</b>	Signal degrade BER threshold. The default is 6.
<b>sf-ber</b>	Signal failure BER threshold. The default is 3 (10e-3).
<i>rate</i>	Bit-error rate from 3 to 9 (10-n).

## posi framing-sdh

The **posi framing-sdh** command is replaced by the **pos framing** command. See the description of the **pos framing** command for more information.

## pri-group

To specify ISDN PRI on a channelized E1 or T1 card on a Cisco 7500 series router, use the **pri-group** command in controller configuration mode. To remove the ISDN PRI, use the **no** form of this command.

**pri-group** [*timeslots range*]

**no pri-group**

Syntax Description	<i>timeslots range</i>	(Optional) Specifies a single range of values from 1 to 23.
--------------------	------------------------	---

## pulse-time

To enable pulsing data terminal ready (DTR) signal intervals on the serial interfaces, use the **pulse-time** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

**pulse-time** *seconds*

**no pulse-time**

Syntax Description	<i>seconds</i>	Integer that specifies the DTR signal interval in seconds. The default is 0.
--------------------	----------------	--

## ring-speed

To set the ring speed for the CSC-1R and CSC-2R Token Ring interfaces, use the **ring-speed** command in interface configuration mode.

**ring-speed** *speed*

Syntax Description	<i>speed</i>	Integer that specifies the ring speed, either 4 for 4-Mbps operation or 16 for 16-Mbps operation. The default is 16.
--------------------	--------------	--

## scramble

To enable scrambling of the payload on the PA-E3 and PA-T3 port adapters, use the **scramble** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

**scramble**

**no scramble**

Syntax Description	This command has no arguments or keywords.
--------------------	--

## sdhc cts-delay

The **sdhc cts-delay** command is replaced by the **half-duplex timer** command. See the description of the **half-duplex timer** command in this chapter for more information.

## sdhc hdx

The **sdhc hdx** command is replaced by the **half-duplex** command. See the description of the **half-duplex** command in this chapter for more information.

## sdhc rts-delay

The **sdhc rts-delay** command is replaced by the **half-duplex timer** command. See the description of the **half-duplex timer** command in this chapter for more information.

## service-module 56k clock rate

To configure the network line speed for a serial interface on a 4-wire, 56/64-kbps CSU/DSU module, use the **service-module 56k clock rate** command in interface configuration mode. To enable a network line speed of 56 kbps, which is the default, use the **no** form of this command.

**service-module 56k clock rate** *speed*

**no service-module 56k clock rate** *speed*

---

### Syntax Description

<i>speed</i>	Network line speed in kbps. The default speed is 56 kbps. Choose from one of the following optional speeds: <ul style="list-style-type: none"> <li>• <b>2.4</b>—2400 kbps</li> <li>• <b>4.8</b>—4800 kbps</li> <li>• <b>9.6</b>—9600 kbps</li> <li>• <b>19.2</b>—19200 kbps</li> <li>• <b>38.4</b>—38400 kbps</li> <li>• <b>56</b>—56000 kbps</li> <li>• <b>64</b>—64000 kbps</li> <li>• <b>auto</b>—Automatic line speed mode. Configure this option if your line speed is constantly changing.</li> </ul>
--------------	---

---

## service-module 56k clock source

To set up the clock source on a serial interface for a 4-wire, 56/64-kbps CSU/DSU module, use the **service-module 56k clock source** command in interface configuration mode. To specify that the clocking come from line, use the **no** form of this command.

```
service-module 56k clock source {line | internal}
```

```
no service-module 56k clock source {line | internal}
```

Syntax Description	line	internal
	Uses the clocking provided by the active line coming in to the router. This is the default.	Uses the internal clocking provided by the hardware module.

## service-module 56k data-coding

To prevent application data from replicating loopback codes when operating at 64 kbps on a 4-wire CSU/DSU, use the **service-module 56k data-coding** command in interface configuration mode. To enable normal transmission, use the **no** form of this command.

```
service-module 56k data-coding {normal | scrambled}
```

```
no service-module 56k data-coding {normal | scrambled}
```

Syntax Description	normal	scrambled
	Specifies normal transmission of data. This is the default.	Scrambles bit codes or user data before transmission. All control codes such as out-of-service and out-of-frame are avoided.

## service-module 56k network-type

To transmit packets in switched dial-up mode or digital data service (DDS) mode using a serial interface on a 4-wire, 56/64-kbps CSU/DSU module, use the **service-module 56k network-type** command in interface configuration mode. To transmit from a dedicated leased line in DDS mode, use the **no** form of this command.

```
service-module 56k network-type {dds | switched}
```

```
no service-module 56k network-type {dds | switched}
```

Syntax Description	dds	switched
	Transmits packets in DDS mode or through a dedicated leased line. The default is DDS enabled for the 4-wire CSU/DSU.	Transmits packets in switched dial-up mode. On a 2-wire, switched 56-kbps CSU/DSU module, this is the default and only setting.

## service-module 56k remote-loopback

To enable the acceptance of a remote loopback request on a serial interface on a 2- or 4-wire, 56/64-kbps CSU/DSU module, use the **service-module 56k remote-loopback** command in interface configuration mode. To disable the module from entering loopback, use the **no** form of this command.

```
service-module 56k remote-loopback
```

```
no service-module 56k remote-loopback
```

**Syntax Description** This command has no arguments or keywords.

## service-module 56k switched-carrier

To select a service provider to use with a 2- or 4-wire, 56/64-kbps dial-up serial line, use the **service-module 56k switched-carrier** command in interface configuration mode. To enable the default service provider, use the **no** form of this command.

```
service-module 56k switched-carrier {att | sprint | other}
```

```
no service-module 56k switched-carrier {att | sprint | other}
```

Syntax Description	att	AT&T or other digital network service provider. This is the default on the 4-wire, 56/64-kbps CSU/DSU module.
	sprint	Sprint or other service provider whose network requires echo cancelers. This is the default on the 2-wire, switched 56-kbps CSU/DSU module.
	other	Any other service provider.

## service-module t1 clock source

To specify the clock source for the fractional T1/T1 CSU/DSU module, use the **service-module t1 clock source** command in interface configuration mode. To return to the default line clock, use the **no** form of this command.

```
service-module t1 clock source {internal | line}
```

```
no service-module t1 clock source {internal | line}
```

Syntax Description	internal	Specifies the CSU/DSU internal clock.
	line	Specifies the line clock. This is the default.

## service-module t1 data-coding

To guarantee the ones density requirement on an alternate mark inversion (AMI) line using the fractional T1/T1 module, use the **service-module t1 data-coding** command in interface configuration mode. To enable normal data transmission, use the **no** form of this command.

```
service-module t1 data-coding {inverted | normal}
```

```
no service-module t1 data-coding {inverted | normal}
```

Syntax Description	inverted	Inverts bit codes by changing all 1 bits to 0 bits and all 0 bits to 1 bits.
	normal	Requests that no bit codes be inverted before transmission. This is the default.

## service-module t1 fdl

To set the FDL parameter to either ATT or ANSI, use the **service-module t1 fdl** command in interface configuration mode. To ignore the FDL parameter, use the **no** form of this command.

```
service-module t1 fdl {ansi | att}
```

```
no service-module t1 fdl
```

Syntax Description	ansi	Sets the FDL parameter to ANSI.
	att	Sets the FDL parameter to ATT.

## service-module t1 framing

To select the frame type for a line using the fractional T1/T1 (FT1/T1) module, use the **service-module t1 framing** command in interface configuration mode. To revert to the default, Extended Super Frame, use the **no** form of this command.

```
service-module t1 framing {esf | sf}
```

```
no service-module t1 framing {esf | sf}
```

Syntax Description	esf	Specifies Extended Super Frame as the T1 frame type. This is the default.
	sf	Specifies D4 Super Frame as the T1 frame type.

## service-module t1 lbo

To configure the CSU line-build-out (LBO) on a fractional T1/T1 CSU/DSU module, use the **service-module t1 lbo** command in interface configuration mode. To disable line-build-out, use the **no** form of this command.

```
service-module t1 lbo {-15 db | -7.5 db | none}
```

```
no service-module t1 lbo {-15 db | -7.5 db | none}
```

### Syntax Description

<b>-15 db</b>	Decreases outgoing signal strength by 15 dB.
<b>-7.5 db</b>	Decreases outgoing signal strength by 7.5 dB.
<b>none</b>	Transmits packets without decreasing outgoing signal strength.

## service-module t1 linecode

To select the line code for the fractional T1/T1 module, use the **service-module t1 linecode** command in interface configuration mode. To select the default, the B8ZS line code, use the **no** form of this command.

```
service-module t1 linecode {ami | b8zs}
```

```
no service-module t1 linecode {ami | b8zs}
```

### Syntax Description

<b>ami</b>	Specifies alternate mark inversion (AMI) as the line code.
<b>b8zs</b>	Specifies binary 8 zero substitution (B8ZS) as the line code. This is the default.

## service-module t1 remote-alarm-enable

To generate remote alarms (yellow alarms) at the local CSU/DSU or detect remote alarms sent from the remote CSU/DSU, use the **service-module t1 remote-alarm-enable** command in interface configuration mode. To disable remote alarms, use the **no** form of this command.

```
service-module t1 remote-alarm-enable
```

```
no service-module t1 remote-alarm-enable
```

### Syntax Description

This command has no arguments or keywords.

## service-module t1 remote-loopback

To specify if the fractional T1/T1 CSU/DSU module enters loopback mode when it receives a loopback code on the line, use the **service-module t1 remote-loopback** command in interface configuration mode. To disable remote loopbacks, use the **no** form of this command.

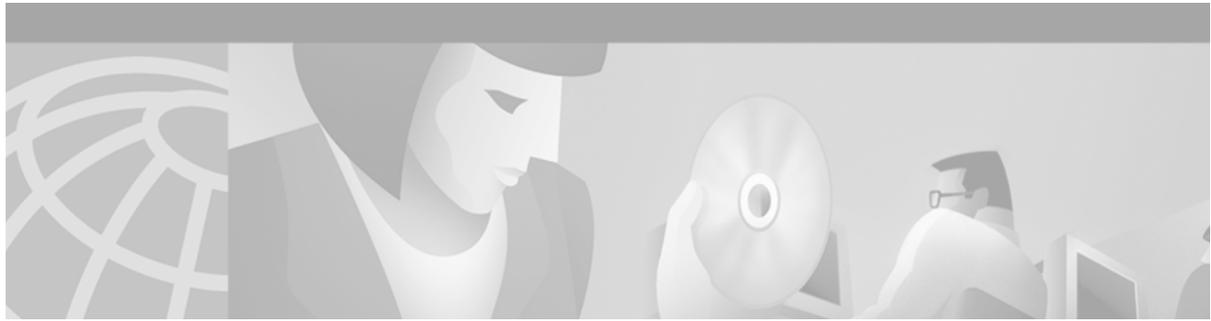
```
service-module t1 remote-loopback {full | payload} [alternate | v54]
```

```
no service-module t1 remote-loopback {full | payload}
```

### Syntax Description

<b>full</b>	Configures the remote loopback code used to transmit or accept CSU loopback requests. This is the default, along with <b>payload</b> .
<b>payload</b>	Configures the loopback code used by the local CSU/DSU to generate or detect payload-loopback commands. This is the default, along with <b>full</b> .
<b>alternate</b>	(Optional) Transmits a remote CSU/DSU loopback request using a 4-in-5 pattern for loopup and a 2-in-3 pattern for loopdown. This is an inverted version of the standard loopcode request.
<b>v54</b>	(Optional) Industry standard loopback code. Use this configuration for CSU/DSUs that may not support the Accunet loopup standards. This keyword is used only with a <b>payload</b> request, not a <b>full</b> request.

■ service-module t1 remote-loopback



## Interface Commands: service-module t1 timeslots Through yellow

---

This chapter describes the function and syntax of the interface commands: **service-module t1 timeslots** through **yellow**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Interface Command Reference*.

### service-module t1 timeslots

To define time slots that constitute a fractional T1/T1 (FT1/T1) channel, use the **service-module t1 timeslots** command in interface configuration mode. To resume the default setting (all FT1/T1 time slots transmit at 64 kbps), use the **no** form of this command.

```
service-module t1 timeslots {range | all} [speed {56 | 64}]
```

```
no service-module t1 timeslots {range | all}
```

Syntax Description	
<i>range</i>	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.
<b>all</b>	Selects all FT1/T1 time slots.
<b>speed</b>	(Optional) Specifies the time slot speed.
<b>56</b>	(Optional) 56 kbps.
<b>64</b>	(Optional) 64 kbps. This is the default.

## service single-slot-reload-enable

To enable single line card reloading for all line cards in the Cisco 7500 series router, use the **service single-slot-reload-enable** command in global configuration mode. To disable single line card reloading for the line cards in the Cisco 7500 series router, use the **no** form of this command.

**service single-slot-reload-enable**

**no service single-slot-reload-enable**

---

**Syntax Description** This command has no arguments or keywords.

## show aps

To display information about the current automatic protection switching (APS) feature, use the **show aps** command in privileged EXEC mode.

**show aps**

---

**Syntax Description** This command has no arguments or keywords.

## show compress

To display compression statistics, use the **show compress** command in EXEC mode.

**show compress**

---

**Syntax Description** This command has no arguments or keywords.

## show controllers cbus

To display all information under the cBus controller card, use the **show controllers cbus** command in privileged EXEC mode on the Cisco 7500 series routers. This command also shows the capabilities of the card and reports controller-related failures.

**show controllers cbus**

---

**Syntax Description** This command has no arguments or keywords.

## show controllers ethernet

To display information on the Cisco 2500, Cisco 3000, or Cisco 4000 series routers, use the **show controllers ethernet** command in EXEC mode.

```
show controllers ethernet number
```

Syntax Description	<i>number</i>
	Interface number of the Ethernet interface.

## show controllers fastethernet

To display information about initialization block, transmit ring, receive ring and errors for the Fast Ethernet controller chip on the Cisco 4500, Cisco 7200 series, or Cisco 7500 series routers, use the **show controllers fastethernet** command in EXEC mode.

### Cisco 4500 Series

```
show controllers fastethernet number
```

### Cisco 7200 Series

```
show controllers fastethernet slot/port
```

### Cisco 7500 Series

```
show controllers fastethernet slot/port-adapter/port
```

Syntax Description	<i>number</i>
	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
	<i>slot</i>
	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>
	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>
	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## show controllers fddi

To display all information under the FDDI Interface Processor (FIP) on the Cisco 7200 series and Cisco 7500 series routers, use the **show controllers fddi** command in user EXEC mode.

```
show controllers fddi
```

---

**Syntax Description** This command has no arguments or keywords.

## show controllers gigabitethernet

To display initialization block information, transmit ring, receive ring, and errors for the Gigabit Ethernet interface controllers of the Cisco 7200-I/O-GE+E, use the **show controllers gigabitethernet** command in privileged EXEC mode.

```
show controllers gigabitethernet slot/port
```

---

<b>Syntax Description</b>	<i>slot</i>	Slot number on the interface.
	<i>port</i>	Port number on the interface.

---

## show controllers lex

To show hardware and software information about the LAN Extender chassis, use the **show controllers lex** command in EXEC mode.

```
show controllers lex [number]
```

### Cisco 7500 Series

```
show controllers lex [slot/port]
```

---

<b>Syntax Description</b>	<i>number</i>	(Optional) Number of the LAN Extender interface about which to display information.
	<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.

---

## show controllers mci

To display all information under the Multiport Communications Interface (MCI) card or the SCI, use the **show controllers mci** command in privileged EXEC mode.

```
show controllers mci
```

---

**Syntax Description** This command has no arguments or keywords.

## show controllers pibus

To display all information about the bus interface, use the **show controllers pibus** command in privileged EXEC mode.

```
show controllers pibus
```

---

**Syntax Description** This command has no arguments or keywords.

## show controllers pos

To display information about the POS (Packet-Over-SONET) controllers, use the **show controllers pos** command in privileged EXEC mode.

```
show controllers pos [slot-number] [details]
```

---

<b>Syntax Description</b>	<i>slot-number</i>	(Optional) The chassis slot that contains the POS interface. For the Cisco 7500 series routers, use slot/port adapter/port (for example, 2/0/0). For the Cisco 12000 series routers, use slot/port (for example, 4/0). The “/” is required. If you do not specify a slot number, information for all the installed POS controllers is displayed.
	<b>details</b>	(Optional) In addition to the normal information displayed by the <b>show controllers pos</b> command, the details keyword provides a hexadecimal and ASCII “dump” of the path trace buffer.

---

## show controllers serial

To display information that is specific to the interface hardware, use the **show controllers serial** command in privileged EXEC mode.

```
show controllers serial [slot/port]
```

### Cisco 7500 Series and Cisco 7000 Series with the RSP7000 and RSP7000CI

```
show controllers serial [slot/port-adapter/port]
```

Syntax Description	slot	(Optional) Slot number of the interface.
	port	(Optional) Port number on the interface. The port value is always 0.
	port-adapter	(Optional) On Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI, the location of the port adapter on a VIP. The value can be 0 or 1.

## show controllers t1

To display information about the T1 links or to display the hardware and software driver information for the T1 controller, use the **show controllers t1** command in privileged EXEC mode.

### Cisco 7500 Series

```
show controllers t1 [slot/port]
```

### Cisco 4000 Series

```
show controllers t1 number
```

### Cisco AS5800 Access Servers

```
show controller t1 dial-shelf/slot/t3-port:t1-num
```

Syntax Description	slot/port	(Optional) Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific slot and port numbers.
	number	Network processor number (NPM) number, in the range 0 through 2.
	dial-shelf	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
	slot	Location of the CT3 interface card in the dial shelf chassis.
	t3-port	T3 port number. The only valid value is 0.
	:t1-num	T1 time slot in the T3 line. The value can be from 1 to 28.

## show controllers t1 bert

To get the results of the bit-error rate testing (BERT) run for all ports, use the **show controllers t1 bert** command in privileged EXEC mode.

```
show controllers {type} [controller-number] [bert]
```

Syntax Description		
<i>type</i>		Specify either T1 or E1 facility.
<i>controller-number</i>		(Optional) Select a specific controller/port numbers. The range is 0 to 7. If not selected, the display will show all ports.
<b>bert</b>		(Optional) Type <b>bert</b> to get a specific display for the BERT results. Otherwise, the display will include all other non-BERT information.

## show controllers t3

To display information about the Channelized T3 Interface Processor (CT3IP) on Cisco 7500 series routers or to display hardware and software driver information for a T3 controller on Cisco AS5800 access servers, use the **show controllers t3** command in privileged EXEC mode.

### Cisco 7500 Series Routers

```
show controllers t3 [slot/port-adapter/port [:t1-channel]] [brief | tabular | remote performance  
[brief | tabular]]
```

### Cisco AS5800 Access Servers

```
show controllers t3 dial-shelf/slot/t3-port
```

Syntax Description		
<i>slot</i>		(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>		(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
<i>port</i>		(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>:t1-channel</i>		(Optional) For the CT3IP, the T1 channel is a number between 1 and 28.
<b>brief</b>		(Optional) Displays a subset of information.
<b>tabular</b>		(Optional) Displays information in a tabular format.
<b>remote performance</b>		(Optional) Displays the far-end ANSI performance monitor information when enabled on the T1 channel with the <b>t1 fdl ansi</b> controller command.
<i>dial-shelf</i>		Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
<i>slot</i>		Location of the CT3 interface card in the dial shelf chassis.
<i>t3-port</i>		T3 port number. The only valid value is 0.

## show controllers token

To display information about memory management and error counters on the Token Ring Interface Processor (exTRIP) for the Cisco 7500 series routers, use the **show controllers token** command in privileged EXEC mode.

```
show controllers token
```

---

**Syntax Description** This command has no arguments or keywords.

## show controllers vg-anylan

To display the controller information for the 100VG-AnyLAN port adapter on Cisco 7200 series routers and Cisco 7500 series routers, use the **show controllers vg-anylan** command in user EXEC mode.

### Cisco 7500 Series with VIP Cards

```
show controllers vg-anylan slot/port-adapter/port
```

### Cisco 7200 Series

```
show controllers vg-anylan slot/port
```

---

<b>Syntax Description</b>	<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
	<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.

---

## show diag

To display hardware information for the router, use the **show diag** command in privileged EXEC mode.

```
show diag [slot]
```

---

<b>Syntax Description</b>	<i>slot</i>	(Optional) Slot number of the interface.
---------------------------	-------------	--

---

## show diagbus

To display 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, use the **show diagbus** command in privileged EXEC mode.

```
show diagbus [slot]
```

---

### Syntax Description

<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
-------------	---

---

## show hub

To display information about the hub (repeater) on an Ethernet interface of a Cisco 2505 or Cisco 2507 router, use the **show hub** command in EXEC mode.

```
show hub [ethernet number [port [end-port]]]
```

---

### Syntax Description

<b>ethernet</b>	(Optional) Indicates that this is an Ethernet hub.
<i>number</i>	(Optional) Hub number, starting with 0. Because there is currently only one hub, this number is 0.
<i>port</i>	(Optional) Port number on the hub. On the Cisco 2505 router, port numbers range from 1 through 8. On the Cisco 2507 router, port numbers range from 1 through 16. If a second port number follows, this port number indicates the beginning of a port range.
<i>end-port</i>	(Optional) Ending port number of a range.

---

## show interfaces

To display statistics for all interfaces configured on the router or access server, use the **show interfaces** command in privileged EXEC mode. The resulting output varies, depending on the network for which an interface has been configured.

```
show interfaces [type number] [first] [last] [accounting]
```

### Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor

```
show interfaces [type slot/port] [accounting]
```

### Cisco 7500 Series with Ports on VIPs

```
show interfaces [type slot/port-adapter/port] [ethernet | serial]
```

Syntax Description		
	<i>type</i>	(Optional) Interface type. Allowed values for <i>type</i> include <b>async</b> , <b>bri0</b> , <b>dialer</b> , <b>ethernet</b> , <b>fastethernet</b> , <b>fdi</b> , <b>hssi</b> , <b>loopback</b> , <b>null</b> , <b>serial</b> , <b>tokenring</b> , and <b>tunnel</b> .  For the Cisco 4000 series routers, <i>type</i> can be <b>e1</b> , <b>ethernet</b> , <b>fastethernet</b> , <b>fdi</b> , <b>serial</b> , <b>t1</b> , and <b>token</b> . For the Cisco 4500 series routers, <i>type</i> can also include <b>atm</b> .  For the Cisco 7000 family, <i>type</i> can be <b>atm</b> , <b>e1</b> , <b>ethernet</b> , <b>fastethernet</b> , <b>fdi</b> , <b>serial</b> , <b>t1</b> , and <b>tokenring</b> . For the Cisco 7500 series <i>type</i> can also include <b>pos</b> .
	<i>number</i>	(Optional) Port number on the selected interface.
	<i>first last</i>	(Optional) For the Cisco 2500 and 3000 series routers, ISDN BRI only. The argument <i>first</i> can be either 1 or 2. The argument <i>last</i> can only be 2, indicating B channels 1 and 2.  D-channel information is obtained by using the command without the optional arguments.
	<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that has been sent through the interface.
	<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## show interfaces ctunnel

To display information about an IP over CLNS tunnel (CTunnel), use the **show interfaces ctunnel** command in privileged EXEC mode.

```
show interfaces ctunnel interface-number [accounting]
```

Syntax Description		
	<i>interface-number</i>	Virtual interface number.
	<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

## show interfaces ethernet

To display information about an Ethernet interface on the router, use the **show interfaces ethernet** command in privileged EXEC mode.

```
show interfaces ethernet unit [accounting]
```

### Cisco 7200 and 7500 Series

```
show interfaces ethernet [slot/port] [accounting]
```

### Cisco 7500 Series with Ports on VIPs

```
show interfaces ethernet [type slot/port-adapter/port]
```

Syntax	Description
<i>unit</i>	Must match a port number on the selected interface.
<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>type</i>	(Optional) Type of interface.
<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## show interfaces fastethernet

To display information about the Fast Ethernet interfaces, use the **show interfaces fastethernet** command in EXEC mode.

### Cisco 4500 and 4700 Series

```
show interfaces fastethernet [number]
```

### Cisco 7200 and 7500 Series

```
show interfaces fastethernet [slot/port]
```

### Cisco 7500 Series with a VIP

```
show interfaces fastethernet [slot/port-adapter/port]
```

Syntax Description		
	<i>number</i>	(Optional) Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 series routers, specifies the network interface module (NIM) or NPM number. The numbers are assigned at the factory at the time of installation or when added to a system.
	<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## show interfaces fddi

To display information about the FDDI interface, use the **show interfaces fddi** command in EXEC mode.

**show interfaces fddi** *number* [**accounting**]

### Cisco 7000 and 7200 Series

**show interfaces fddi** [*slot/port*] [**accounting**]

### Cisco 7500 Series

**show interfaces fddi** [*slot/port-adapter/port*] [**accounting**]

Syntax Description		
	<i>number</i>	Port number on the selected interface.
	<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
	<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## show interfaces gigabitethernet

To check the status and configuration settings of the Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E, use the **show interfaces gigabitethernet** command in privileged EXEC mode.

**show interfaces gigabitethernet** *slot/port*

Syntax Description		
	<i>slot</i>	Slot number on the interface.
	<i>port</i>	Port number on the interface.

## show interfaces hssi

To display information about the high-speed serial interface (HSSI), use the **show interfaces hssi** command in privileged EXEC mode.

```
show interfaces hssi unit [accounting]
```

### Cisco 7500 Series

```
show interfaces hssi [slot/port] [accounting]
```

Syntax Description		
	<i>unit</i>	Must match a port number on the selected interface.
	<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
	<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.

## show interfaces ip-brief

To display a brief summary of the information and status for an IP address, use the **show interfaces ip-brief** command in EXEC mode.

```
show interfaces ip-brief
```

Syntax Description	
	This command has no arguments or keywords.

## show interfaces lex

To display statistics about a LAN Extender interface, use the **show interfaces lex** command in EXEC mode.

```
show interfaces lex number [ethernet | serial]
```

Syntax Description		
	<i>number</i>	Number of the LAN Extender interface that resides on the core router about which to display statistics.
	<b>ethernet</b>	(Optional) Displays statistics about the Ethernet interface that resides on the LAN Extender chassis.
	<b>serial</b>	(Optional) Displays statistics about the serial interface that resides on the LAN Extender chassis.

## show interfaces loopback

To display information about the loopback interface, use the **show interfaces loopback** command in privileged EXEC mode.

```
show interfaces loopback [number] [accounting]
```

Syntax Description		
	<i>number</i>	(Optional) Port number on the selected interface.
	<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

## show interfaces port-channel

To display the information about the Fast EtherChannel on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the RSP7000 and RSP7000CI, use the **show interfaces port-channel** command in EXEC mode.

```
show interfaces port-channel [channel-number]
```

Syntax Description		
	<i>channel-number</i>	(Optional) Port channel number. Range is 1 to 4.

## show interfaces pos

To display information about the Packet OC-3 interface in Cisco 7500 series routers, use the **show interfaces pos** command in EXEC mode.

### Cisco 7000 and 7500 Series with VIPs

```
show interfaces pos [slot/port-adapter/port]
```

Syntax Description		
	<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
	<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.

## show interfaces posi

The **show interfaces posi** command is replaced by the **show interfaces pos** command. See the description of the **show interfaces pos** command for more information.

# show interfaces serial

To display information about a serial interface, use the **show interfaces serial** command in privileged EXEC mode. When using Frame Relay encapsulation, use the **show interfaces serial** command in EXEC mode to display information about the multicast data-link connection identifier (DLCI), the DLCIs used on the interface, and the DLCI used for the Local Management Interface (LMI).

## Cisco 4000 Series

```
show interfaces serial [number [:channel-group]] [accounting]
```

## Cisco 7200 Series

```
show interfaces serial [slot/port] [accounting]
```

## Cisco 7000 and Cisco 7500 Series with the RSP7000, RSP7000CI, or Ports on VIPs

```
show interfaces serial [slot/port-adapter/port]
```

## Cisco 7500 Series

```
show interfaces serial [slot/port [:channel-group]] [accounting]
```

## Cisco 7500 Series with a CT3IP

```
show interfaces serial [slot/port-adapter/port] [:t1-channel] [accounting | crb]
```

## Cisco AS5800 Access Servers

```
show interfaces serial dial-shelf[slot]t3-port:t1-num:chan-group
```

### Syntax Description

<i>number</i>	(Optional) Number of the port being configured.
<i>:channel-group</i>	(Optional) On the Cisco 4000 series with an NPM or Cisco 7500 series routers with a MIP (MultiChannel Interface Processor), specifies the T1 channel-group number in the range of 0 to 23 defined with the <b>channel-group</b> controller configuration command.
<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
<i>:t1-channel</i>	(Optional) For the CT3IP, the T1 channel is a number between 1 and 28.  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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

<b>crb</b>	(Optional) Shows interface routing and bridging information.
<i>dial-shelf</i>	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
<i>slot</i>	Location of the CT3 interface card in the dial shelf chassis.
<i>t3-port</i>	T3 port number. The only valid value is 0.
<i>:t1-num</i>	T1 time slot in the T3 line. The value can be from 1 to 28.
<i>:chan-group</i>	Channel group identifier.

## show interfaces tokenring

To display information about the Token Ring interface and the state of source route bridging, use the **show interfaces tokenring** command in privileged EXEC mode.

```
show interfaces tokenring unit [accounting]
```

### Cisco 7200 and 7500 Series

```
show interfaces tokenring slot/port [accounting]
```

### Cisco 7500 Series with Ports on VIPs

```
show interfaces tokenring [slot/port-adapter/port]
```

### Syntax Description

<i>unit</i>	Must match the interface port line number.
<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
<i>slot</i>	On the Cisco 7000 series routers, slot location of the interface processor. On the Cisco 7000, the value can be 0, 1, 2, 3, or 4. On the Cisco 7010, value can be 0, 1, or 2.  On the Cisco 7200 series routers, slot location of the port adapter; the value can be 1, 2, 3, 4, 5, or 6.
<i>port</i>	Port number on the interface. On the Cisco 7000 series routers this argument is required, and the values can be 0, 1, 2, or 3.  (Optional) For the VIP this argument is optional, and the port value can be 0, 1, 2, or 3 for 4-port Token Ring interfaces.  On the Cisco 7200 series routers, the number depends on the type of port adapter installed.
<i>port-adapter</i>	(Optional) On the Cisco 7000 series and Cisco 7500 series routers, specifies the ports on a VIP. The value can be 0 or 1.

## show interfaces tunnel

To list tunnel interface information, use the **show interfaces tunnel** command in privileged EXEC mode.

```
show interfaces tunnel number [accounting]
```

Syntax Description		
	<i>number</i>	Port line number.
	<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

## show interfaces vg-anylan

To display the information about the 100VG-AnyLAN port adapter on Cisco 7200 series routers and Cisco 7500 series routers, use the **show interfaces vg-anylan** command in EXEC mode.

### Cisco 7200 Series

```
show interfaces vg-anylan [slot/port]
```

### Cisco 7500 Series with VIPs

```
show interfaces vg-anylan [slot/port-adapter/port]
```

Syntax Description		
	<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	(Optional) Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## show ip director dfp

To display information about the current status of the DistributedDirector connections with a particular Dynamic Feedback Protocol (DFP) agent, use the **show ip director dfp** command in EXEC mode.

```
show ip director dfp [host-name | ip-address]
```

Syntax Description		
	<i>host-name</i>	(Optional) Host name.
	<i>ip-address</i>	(Optional) IP address.

## show pas caim

To show debug information about the data compression Advanced Interface Module (CAIM) daughtercard, use the **show pas caim** command in EXEC mode.

```
show pas caim {rings | dma | coprocessor | stats | cnxt_table | page_table} element-number
```

Syntax	Description
<b>rings</b> <i>element-number</i>	Displays current content of the Direct Memory Access (DMA) ring buffer.
<b>dma</b> <i>element-number</i>	Displays registers of the Jupiter DMA controller.
<b>coprocessor</b> <i>element-number</i>	Displays registers of the Hifn 9711 compression coprocessor.
<b>stats</b> <i>element-number</i>	Displays statistics describing operation of the data compression Advanced Interface Module (AIM).
<b>cnxt_table</b> <i>element-number</i>	Displays the context of the specific data compression AIM element.
<b>page_table</b> <i>element-number</i>	Displays the page table for each CAIM element.

## show pas eswitch address

To display the Layer 2 learned addresses for an interface, use the **show pas eswitch address** command in EXEC mode.

```
show pas eswitch address [ethernet | fastethernet] [slot/port]
```

Syntax	Description
<b>ethernet</b>   <b>fastethernet</b>	(Optional) Type of interface.
<i>slot</i>	(Optional) Slot number of the interface.
<i>port</i>	(Optional) Interface number.

## show pci aim

To show the IDPROM contents for each compression Advanced Interface Module (AIM) daughtercard in the Cisco 2600 router, use the **show pic aim** command in EXEC mode.

```
show pci aim
```

Syntax	Description
<b>show pci aim</b>	This command has no arguments or keywords.

## show service-module serial

To display the performance report for an integrated CSU/DSU, use the **show service-module serial** command in privileged EXEC mode.

```
show service-module serial number [performance-statistics [interval-range]]
```

Syntax Description	
<i>number</i>	Interface number 0 or 1.
<b>performance-statistics</b>	(Optional) Displays the CSU/DSU performance statistics for the past 24 hours. This keyword applies only to the fractional T1/T1 module.
<i>interval-range</i>	(Optional) Specifies the number of 15-minute intervals displayed. 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.

## show smf

To display the configured software MAC address filter (SMF) on various interfaces of a router, use the **show smf** command in EXEC mode.

```
show smf [interface-name]
```

Syntax Description	
<i>interface-name</i>	(Optional) Displays information about the specified interface. Choices can include atm, ethernet, fastethernet, null, serial, tokenring, and async.

## show tdm backplane

To display modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the time-division multiplexing (TDM) assignment, use the **show tdm backplane** command in privileged EXEC mode.

```
show tdm backplane {stream stream-number}
```

Syntax Description	
<b>stream</b>	Backplane stream in the range 0 to 7. There are 8 backplane “streams” on the TDM backplane for the Cisco AS5300 access server. Each stream runs at 2 MHz and has 32 channels (running at 64 Hz) on the Cisco AS5300 access server backplane hardware.
<i>stream-number</i>	Actual number entered (either 0 to 7 or 0 to 15). An actual number needs to be entered.

## show tdm connections

To display a snapshot of the time-division multiplexing (TDM) bus connection memory in a Cisco AS5200 access server or to display information about the connection memory programmed on the Mitel TDM chip in a Cisco AS5800 access server, use the **show tdm connections** command in privileged EXEC mode.

### Cisco AS5200 Access Server

```
show tdm connections [motherboard | slot slot-number]
```

### Cisco AS5800 Access Server

```
show tdm connections {motherboard {stream stream-number} | slot slot-number {device device-number {stream stream-number}}}
```

#### Syntax Description

<b>motherboard</b>	<p><b>Cisco AS5200 Access Server</b></p> <p>(Optional) Motherboard in the Cisco AS5200 access server.</p> <p><b>Cisco AS5800 Access Server</b></p> <p>Motherboard in the Cisco AS5800 access server has ethernet and serial interfaces, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco 5300 access server.</p>
<b>slot slot-number</b>	<p><b>Cisco AS5200 Access Server</b></p> <p>(Optional) Number of the slot being configured.</p> <p><b>Cisco AS5800 Access Server</b></p> <p>There are 3 slots on the Cisco AS5800 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted into each slot. Each card in the slot has one or two TDM devices (either MT8980 or MT90820) on them.</p>
<b>stream</b>	<p>Device stream in the range 0 to 7. There are 8 backplane “streams” on the TDM backplane for the Cisco AS5800 access server. Each stream runs at 2 Mhz and has 32 channels (running at 64 Hz) on the Cisco AS5800 access server backplane hardware.</p>
<i>stream-number</i>	<p>Stream number (the range is 0 to 7 or 0 to 15).</p>
<b>device</b>	<p>TDM device on the motherboard or slot cards. The range for the Cisco AS5800 access server is 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and some of the slot cards have two devices (for example, the Octal PRI has two MT90820 TDM devices). The TDM device is also referred to as “TSI Chip Number” in the online help.</p>
<i>device-number</i>	<p>Valid range is 0 to 1.</p>

## show tdm data

To display a snapshot of the time-division multiplexing (TDM) bus data memory in a Cisco AS5200 access server or to display data memory that is programmed on the Mitel TDM chip in a Cisco 5800 access server, use the **show tdm data** command in privileged EXEC mode.

### Cisco AS5200 Access Server

```
show tdm data [motherboard | slot slot-number]
```

### Cisco AS5800 Access Server

```
show tdm data { motherboard { stream stream-number } | slot slot-number { device
device-number { stream stream-number } } }
```

Syntax	Description
<b>motherboard</b>	<p><b>Cisco AS5200 Access Server</b></p> <p>(Optional) Motherboard in the Cisco AS5200 access server.</p> <p><b>Cisco AS5800 Access Server</b></p> <p>Motherboard on the Cisco AS5300 access server has the ethernet I/Fs, serial I/Fs, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco AS5300 access server.</p>
<b>slot</b> <i>slot-number</i>	<p><b>Cisco AS5200 Access Server</b></p> <p>(Optional) Number of the slot being configured.</p> <p><b>Cisco AS5800 Access Server</b></p> <p>In addition to the motherboard, there are three slots on the Cisco AS5300 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card in the slot has one or two TDM devices (either MT8980 or MT90820) on them.</p>
<b>stream</b>	<p>TDM device stream in the range 0 to 15. There are up to 16 streams on a TDM device (Mitel 90820). The TDM device is also known as the TSI chip. The help on the command (by typing ?) indicates whether the stream is “Stream number within the TSI chip” or “Backplane Stream.”</p>
<i>stream-number</i>	<p>Stream number within the range of either 0 to 7 or 0 to 15.</p>
<b>device</b>	<p>TDM device on the motherboard, or slot cards. Valid range for the Cisco AS5300 access server is 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to as TSI Chip Number in the help pages.</p>
<i>device-number</i>	<p>Valid range is 0 to 1.</p>

## show tdm detail

To display details about a specific time-division multiplexing (TDM) channel programmed on the Mitel chip, use the **show tdm detail** command in privileged EXEC mode.

**show tdm detail** *slot-number/device-number source-stream-number/source-channel-number*

Syntax	Description
<i>slot-number</i>	There are three slots on the Cisco AS5300 access server. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it. The valid range is 0 to 2.
<i>device-number</i>	TDM device on the motherboard or slot cards. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to a TSI Chip Number in the online help. The valid range is 0 to 1.
<i>source-stream-number</i>	Source stream number from the TDM device. The valid range is 0 to 15.
<i>source-channel-number</i>	Source channel from the TDM device stream. The valid range is 0 to 31.

## show tdm information

To display information about the specified time-division multiplexing (TDM) device, use the **show tdm information** command in privileged EXEC mode.

**show tdm information** { **motherboard** | **slot** *slot-number* { **device** *device-number* } }

Syntax	Description
<b>motherboard</b>	Motherboard on the Cisco AS5300 access server has the ethernet I/Fs, serial I/Fs, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco AS5300 access server.
<b>slot</b>	There are three slots on the Cisco AS5300 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it.
<i>slot-number</i>	Valid range is 0 to 2.
<b>device</b>	TDM device on the motherboard or slot cards. The valid range is 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to as TSI Chip Number in the online help.
<i>device-number</i>	Valid range is 0 to 1.

## show tdm pool

To display time-division multiplexor (TDM) resources available for the specified TDM device, use the **show tdm pool** command in privileged EXEC mode.

```
show tdm pool [slot slot-number]
```

Syntax	Description
<b>slot</b>	(Optional) There are three slots on the Cisco AS5300 access server with a range of 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it.
<i>slot-number</i>	(Optional) Valid range is 0 to 2 for the Cisco AS5300 access server.

## shutdown (controller)

To disable the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **shutdown** command in controller configuration mode. To restart a disabled CT3IP, use the **no** form of this command.

```
shutdown
```

```
no shutdown
```

Syntax	Description
	This command has no arguments or keywords.

## shutdown (hub)

To shut down a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **shutdown** command in hub configuration mode. To restart the disabled hub, use the **no** form of this command.

```
shutdown
```

```
no shutdown
```

Syntax	Description
	This command has no arguments or keywords.

## shutdown (interface)

To disable an interface, use the **shutdown** command in interface configuration mode. To restart a disabled interface, use the **no** form of this command.

**shutdown**

**no shutdown**

---

**Syntax Description** This command has no arguments or keywords.

## smt-queue-threshold

To set the maximum number of unprocessed FDDI station management (SMT) frames that will be held for processing, use the **smt-queue-threshold** command in global configuration mode. To restore the queue to the default, use the **no** form of this command.

**smt-queue-threshold** *number*

**no smt-queue-threshold**

---

**Syntax Description** *number* Number of buffers used to store unprocessed SMT messages that are to be queued for processing. Acceptable values are positive integers. The default value is equal to the number of FDDI interfaces installed in the router.

---

## snmp ifindex clear

To clear any previously configured SNMP ifIndex commands issued in interface configuration mode for a specific interface, use the **snmp ifindex clear** command in interface configuration mode.

**snmp ifindex clear**

---

**Syntax Description** This command has no arguments or keywords.

## snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface only, use the **snmp ifindex persist** command in interface configuration mode. To disable ifIndex persistence only on a specific interface, use the **no** form of this command.

**snmp ifindex persist**

**no snmp ifindex persist**

**Syntax Description** This command has no arguments or keywords.

## snmp-server ifindex persist

To globally enable ifIndex values which will remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command in global configuration mode. To globally disable ifIndex persistence, use the **no** form of this command in global configuration mode.

**snmp-server ifindex persist**

**no snmp-server ifindex persist**

**Syntax Description** This command has no arguments or keywords.

## snmp trap illegal-address

To issue an Simple Network Management Protocol (SNMP) trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router, use the **snmp trap illegal-address** command in hub configuration mode. To disable this function, use the **no** form of this command.

**snmp trap illegal-address**

**no snmp trap illegal-address**

**Syntax Description** This command has no arguments or keywords.

## source-address

To configure source address control on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **source-address** command in hub configuration mode. To remove a previously defined source address, use the **no** form of this command.

**source-address** [*mac-address*]

**no source-address**

### Syntax Description

<i>mac-address</i>	(Optional) MAC address in the packets that the hub will allow to access the network.
--------------------	--

## speed

To configure the speed for a Fast Ethernet interface, use the **speed** command in interface configuration mode. To disable a speed setting, use the **no** form of this command.

**speed** {**10** | **100** | **auto**}

**no speed**

### Syntax Description

<b>10</b>	Configures the interface to transmit at 10 Mbps.
<b>100</b>	Configures the interface to transmit at 100 Mbps. This is the default.
<b>auto</b>	Turns on the Fast Ethernet autonegotiation capability. The interface automatically operates at 10 or 100 Mbps depending on environmental factors, such as the type of media and transmission speeds for the peer routers, hubs, and switches used in the network configuration.

## squelch

To extend the Ethernet twisted-pair 10BASE-T capability beyond the standard 100 meters on the Cisco 4000 platform, use the **squelch** command in interface configuration mode. To restore the default, use the **no** form of this command.

**squelch** {**normal** | **reduced**}

**no squelch** {**normal** | **reduced**}

### Syntax Description

<b>normal</b>	Allows normal capability. This is the default.
<b>reduced</b>	Allows extended 10BASE-T capability.

## srp buffer-size

To make adjustments to buffer settings on the receive side for different priority traffic, use the **srp buffer-size** command in interface configuration mode. To disable buffer size configurations use the **no** form of this command.

```
srp buffer-size receive [high | medium]
```

```
no srp buffer-size receive [high | medium]
```

<b>Syntax Description</b>	<i>receive</i>	Allocates synchronous dynamic random-access memory (SDRAM) buffer for incoming packets.
	<i>high   medium</i>	(Optional) Buffer size, in bytes, for high- or medium-priority packets. Any number from 16 to 8192.

## srp deficit-round-robin

To transfer packets from the internal receive buffer to IOS, use the **srp deficit-round-robin** command in interface configuration mode. To disable **srp deficit-round-robin**, use the **no** form of this command.

```
srp deficit-round-robin [input | output] [high | medium | low] [quantum | deficit]
```

```
no srp deficit-round-robin
```

<b>Syntax Description</b>	<i>input   output</i>	(Optional) Either input or output is specified.
	<i>high   medium   low</i>	(Optional) Priority queue level.
	<i>quantum</i>	(Optional) DRR quantum value. Any number from 9216 to 32,767. The default is 9,216.
	<i>deficit</i>	(Optional) DRR deficit value. Any number from 0 to 65,535. The default is 16,384.

## srp loopback

To loop the spatial reuse protocol (SRP) interface on an OC-12c DPTIP, use the **srp loopback** command in interface configuration mode. To remove the loopback, use the **no** form of this command.

```
srp loopback {internal | line} {a | b}
```

```
no srp loopback
```

<b>Syntax Description</b>	<b>internal   line</b>	Sets the loopback toward the network before going through the framer (internal), or loops the payload data toward the network (line).
	<b>a</b>	Loops back the A side of the interface (inner tx, outer rx).
	<b>b</b>	Loops back the B side of the interface (outer tx, inner rx).

## srp priority-map

To set priority mapping for transmitting and receiving packets, use the **srp priority-map** command in interface configuration mode. To disable priority mapping use the **no** form of this command.

```
srp priority-map {receive} {high | medium | low} {transmit} {high | medium}
```

```
no srp priority-map
```

Syntax Description	receive   transmit	Receiving or transmitting.
	high   medium	Mapping for high- or medium-priority packets. Range is between 1 and 8.
	low	Specifies mapping for low-priority packets on the receive side.

## srp random-detect

To configure WRED (weighted RED) parameters on packets received through an spatial reuse protocol (SRP) interface, use the **srp random-detect** command in interface configuration mode. To return the value to the default, use the **no** form of this command.

```
srp random-detect {compute-interval | enable | input | [high | low | medium] |
                  [exponential-weight | precedence]}
```

```
no srp random-detect
```

Syntax Description	compute-interval	Interval in the range of 1 to 128 nanoseconds used to specify the queue depth compute interval.
	enable	Enables WRED.
	input	WRED on packet input path.
	high   low   medium	(Optional) Priority queue level.
	exponential-weight	Queue weight in bits. Any number from 0 to 6.
	precedence	Input queue precedence.

## srp shutdown

To disable the spatial reuse protocol (SRP) interface, use the **srp shutdown** command in interface configuration mode. To restart a disabled interface, use the **no** form of this command.

```
srp shutdown [a | b]
```

```
no srp shutdown [a | b]
```

Syntax Description	a	(Optional) Specifies side A of the SRP interface.
	b	(Optional) Specifies side B of the SRP interface.

## srp tx-traffic-rate

To limit the amount of high-priority traffic that the spatial reuse protocol (SRP) interface can handle, use the **srp tx-traffic-rate** command in interface configuration mode. Use the **no** form of this command to disable transmitted traffic rate.

**srp tx-traffic** *number*

**no srp tx-traffic** *number*

### Syntax Description

<i>number</i>	Range in kilobits per second. The range is 1 to 65535.
---------------	--

## t1

To create a logical T1 controller from each of the specified time slots of the T3 line, use the **t1** command in controller configuration mode. To delete the defined logical controller, use the **no** form of this command.

**t1** *ds1* **controller**

**no t1** *ds1* **controller**

### Syntax Description

<i>ds1</i>	Time slot within the T3 line. The valid time-slot range is from 1 to 28.
------------	--

## t1 bert

To enable or disable a bit error rate tester (BERT) test pattern for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 bert** controller configuration command. To disable a BERT test pattern, use the **no** form of this command.

**t1** *channel* **bert pattern** {**0s** | **1s** | **2<sup>15</sup>** | **2<sup>20</sup>** | **2<sup>23</sup>**} **interval** *minutes*

**no t1** *channel* **bert pattern** {**0s** | **1s** | **2<sup>15</sup>** | **2<sup>20</sup>** | **2<sup>23</sup>**} **interval** *minutes*

### Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>pattern</b>	Specifies the length of the repeating BERT test pattern.
<b>0s</b>	0s—Repeating pattern of zeros (...000...).
<b>1s</b>	1s—Repeating pattern of ones (...111...).
<b>2<sup>15</sup></b>	2 <sup>15</sup> —Pseudorandom repeating pattern that is 32,767 bits in length.
<b>2<sup>20</sup></b>	2 <sup>20</sup> —Pseudorandom repeating pattern that is 1,048,575 bits in length.
<b>2<sup>23</sup></b>	2 <sup>23</sup> —Pseudorandom repeating pattern that is 8,388,607 bits in length.
<b>interval</b> <i>minutes</i>	Specifies the duration of the BERT test. The interval can be a value from 1 to 14,400 minutes.

## t1 clock source

To specify where the clock source is obtained for use by each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 clock source** controller configuration command.

```
t1 channel clock source {internal | line}
```

Syntax Description	channel	Number between 1 and 28 that indicates the T1 channel.
	<b>internal</b>	Specifies that the internal clock source is used. This is the default.
	<b>line</b>	Specifies that the network clock source is used.

## t1 external

To specify that a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers is used as an external port so that the T1 channel can be further multiplexed on the Multichannel Interface Processor (MIP) or other multiplexing equipment, use the **t1 external** controller configuration command. To remove a T1 as an external port, use the **no** form of this command.

```
t1 external channel [cablelength feet] [linecode ami | b8zs]
```

```
no t1 external channel
```

Syntax Description	channel	Number 1, 2, or 3 that indicates the T1 channel.
	<b>cablelength feet</b>	(Optional) Specifies the cable length, in feet, from the T1 channel to the external CSU or MIP. Values are 0 to 655 feet. The default is 133 feet.
	<b>linecode ami   b8zs</b>	(Optional) Specifies the line coding used by the T1. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). The default is B8ZS.

## t1 fdl ansi

To enable the 1-second transmission of the remote performance reports via the Facility Data Link (FDL) per ANSI T1.403 for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 fdl ansi** controller configuration command. To disable the performance report, use the **no** form of this command.

```
t1 channel fdl ansi
```

```
no t1 channel fdl ansi
```

Syntax Description	channel	Number between 1 and 28 that indicates the T1 channel.
--------------------	---------	--

## t1 framing

To specify the type of framing used by the T1 channels on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 framing** controller configuration command.

```
t1 channel framing {esf | sf}
```

Syntax Description	
<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>esf</b>	Specifies that Extended Super Frame (ESF) is used as the T1 framing type. This is the default.
<b>sf</b>	Specifies that Super Frame is used as the T1 framing type.

## t1 linecode

To specify the type of line coding used by the T1 channels on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 linecode** controller configuration command.

```
t1 channel linecode {ami | b8zs}
```

Syntax Description	
<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>ami</b>	Specifies that alternate mark inversion (AMI) line coding is used by the T1 channel.
<b>b8zs</b>	Specifies that bipolar 8 zero suppression (B8ZS) line coding is used by the T1 channel. This is the default.

## t1 test

To break out a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers to the test port for testing, use the **t1 test** controller configuration command. To remove the T1 channel from the test port, use the **no** form of this command.

```
t1 test channel [cablelength feet] [linecode {ami | b8zs}]
```

```
no t1 test channel
```

Syntax Description	
<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>cablelength feet</b>	(Optional) Specifies the cable length from the T1 channel to the external CSU or Multi-Channel Interface Processor (MIP). Values are 0 to 655 feet. The default cable length is 133 feet.
<b>linecode {ami   b8zs}</b>	(Optional) Specifies the line coding format used by the T1 channel. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). The default is B8ZS.

## t1 timeslot

To specify the time slots and data rate used on each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 timeslot** controller configuration command. To remove the configured T1 channel, use the **no** form of this command.

```
t1 channel timeslot range [speed {56 | 64}]
```

```
no t1 channel timeslot
```

### Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<i>range</i>	Specifies the time slots assigned to the T1 channel. The range can be 1 to 24. A dash represents a range of time slots, and a comma separates time slots. For example, 1-10,15-18 assigns time slots 1 through 10 and 15 through 18.
<b>speed {56   64}</b>	(Optional) Specifies the data rate for the T1 channel. Values are 56 kbps or 64 kbps. The default is 64 kbps. The 56-kbps speed is valid only for T1 channels 21 through 28.

## t1 yellow

To enable detection and generation of yellow alarms for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 yellow** controller configuration command. To disable the detection and generation of yellow alarms, use the **no** form of this command.

```
t1 channel yellow {detection | generation}
```

```
no t1 channel yellow {detection | generation}
```

### Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>detection</b>	Detects yellow alarms. This is the default, along with <b>generation</b> .
<b>generation</b>	Generates yellow alarms. This is the default, along with <b>detection</b> .

## test aim eeprom

To test the data compression Advanced Interface Module (AIM) after it is installed in the Cisco 2600 router, use the **test aim eeprom** global configuration command.

```
test aim eeprom
```

### Syntax Description

This command has no arguments or keywords.

## test interface fastethernet

To test the Fast Ethernet interface by causing the interface to ping itself, use the **test interface fastethernet** EXEC command.

```
test interface fastethernet number
```

Syntax Description	<i>number</i>	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 series router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system and are displayed with the <b>show interfaces</b> command.

## test service-module

To perform self-tests on an integrated CSU/DSU serial interface module, such as a 4-wire, 56/64 kbps CSU/DSU, use the **test service-module** privileged EXEC command.

```
test service-module type number
```

Syntax Description	<i>type</i>	Interface type.
	<i>number</i>	Interface number.

## timeslot

To enable framed mode on a serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter, use the **timeslot** interface configuration command. Framed mode allows you to specify a bandwidth for the interface by designating some of the 32 time slots for data and reserving the others for framing (timing). Unframed mode, also known as clear channel, does not reserve any time slots for framing. To restore the interface to unframed mode, use the **no** form of this command or set the start slot to 0.

```
timeslot start-slot stop-slot
```

```
no timeslot
```

Syntax Description	<i>start-slot</i>	First subframe in the major frame. Valid range is 1 to 31 and must be less than or equal to <i>stop-slot</i> .
	<i>stop-slot</i>	Last subframe in the major frame. Valid range is 1 to 31 and must be greater than or equal to <i>start-slot</i> .

## transmit-buffers backing-store

To buffer short-term traffic bursts that exceed the bandwidth of the output interface, use the **transmit-buffers backing-store** interface configuration command. To disable this function, use the **no** form of this command.

**transmit-buffers backing-store**

**no transmit-buffers backing-store**

---

**Syntax Description** This command has no arguments or keywords.

## transmit-clock-internal

To enable the internally generated clock on a serial interface on a Cisco 7200 series or Cisco 7500 series router when a DTE does not return a transmit clock, use the **transmit-clock-internal** interface configuration command. To disable the feature, use the **no** form of this command.

**transmit-clock-internal**

**no transmit-clock-internal**

---

**Syntax Description** This command has no arguments or keywords.

## transmitter-delay

To specify a minimum dead-time after transmitting a packet, use the **transmitter-delay** command in interface configuration mode. To restore the default, use the **no** form of this command.

**transmitter-delay** *delay*

**no transmitter-delay**

---

**Syntax Description** *delay* On the FSIP, high-speed serial interface (HSSI, and) on the IGS router, the minimum number of High-Level Data Link Control (HDLC) flags to be sent between successive packets. On all other serial interfaces and routers, approximate number of microseconds of minimum delay after transmitting a packet. The valid range is 0 to 13,1071. The default is 0.

---

## ts16

To control the use of time slot 16 for data on a G.703 E1 interface or on a E1-G.703/G.704 serial port adapter, use the **ts16** interface configuration command. To restore the default, use the **no** form of this command.

**ts16**

**no ts16**

---

**Syntax Description** This command has no arguments or keywords.

## tunnel checksum

To enable encapsulator-to-decapsulator checksumming of packets on a tunnel interface, use the **tunnel checksum** interface configuration command. To disable checksumming, use the **no** form of this command.

**tunnel checksum**

**no tunnel checksum**

---

**Syntax Description** This command has no arguments or keywords.

## tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** interface configuration command. To remove the destination, use the **no** form of this command.

**tunnel destination** {*hostname* | *ip-address*}

**no tunnel destination**

---

<b>Syntax Description</b>	<i>hostname</i>	Name of the host destination.
	<i>ip-address</i>	IP address of the host destination expressed in decimal in four-part, dotted notation.

---

## tunnel key

To enable an ID key for a tunnel interface, use the **tunnel key** interface configuration command. To remove the ID key, use the **no** form of this command.

**tunnel key** *key-number*

**no tunnel key**

<b>Syntax Description</b>	<i>key-number</i>	Number from 0 to 4,294,967,295 that identifies the tunnel key.
---------------------------	-------------------	--

## tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** interface configuration command. To restore the default, use the **no** form of this command.

**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre ip** | **nos**}

**no tunnel mode**

<b>Syntax Description</b>	<b>aurp</b>	AppleTalk Update Routing Protocol (AURP).
	<b>cayman</b>	Cayman TunnelTalk AppleTalk encapsulation.
	<b>dvmrp</b>	Distance Vector Multicast Routing Protocol.
	<b>eon</b>	EON compatible CLNS tunnel.
	<b>gre ip</b>	Generic route encapsulation (GRE) protocol over IP. This is the default.
	<b>nos</b>	KA9Q/NOS compatible IP over IP.

## tunnel sequence-datagrams

To configure a tunnel interface to drop datagrams that arrive out of order, use the **tunnel sequence-datagrams** interface configuration command. To disable this function, use the **no** form of this command.

**tunnel sequence-datagrams**

**no tunnel sequence-datagrams**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## tunnel source

To set source address for a tunnel interface, use the **tunnel source** interface configuration command. To remove the source address, use the **no** form of this command.

**tunnel source** {*ip-address* | *type number*}

**no tunnel source**

Syntax Description		
	<i>ip-address</i>	IP address to use as the source address for packets in the tunnel.
	<i>type</i>	Interface type.
	<i>number</i>	Specifies the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the <b>show interfaces</b> command.

## tx-queue-limit

To control the number of transmit buffers available to a specified interface on the MCI and SCI cards, use the **tx-queue-limit** interface configuration command.

**tx-queue-limit** *number*

Syntax Description		
	<i>number</i>	Maximum number of transmit buffers that the specified interface can subscribe.

## yellow

To enable generation and detection of yellow alarms, use the **yellow** command in interface configuration mode.

**yellow** {*generation* | *detection*}

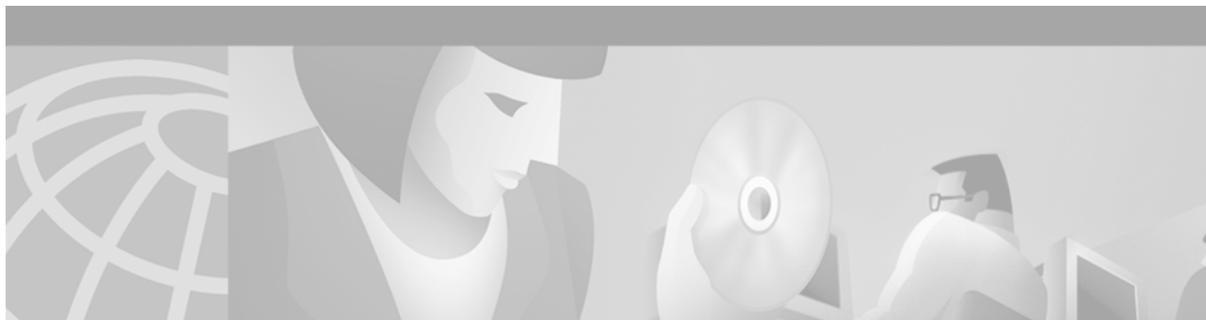
Syntax Description		
	<i>generation</i>	This setting enables or disables generation of yellow alarms.
	<i>detection</i>	This setting enables or disables detection of yellow alarms.

■ yellow



## **Dial Technologies**





## Dial Technologies Commands: aaa authorization configuration default Through ds0-group

This chapter describes the function and syntax of the dial technologies commands: **aaa authorization configuration default** through **ds0-group**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Dial Technologies Command Reference*.

### aaa authorization configuration default

To download static route configuration information from the authorization, authentication, and accounting (AAA) server using TACACS+ or RADIUS, use the **aaa authorization configuration default** global configuration command. To remove static route configuration information, use the **no** form of this command.

```
aaa authorization configuration default {radius | tacacs+}
```

```
no aaa authorization configuration default
```

Syntax Description	radius	RADIUS static route download.
	tacacs+	TACACS+ static route download.

	radius	RADIUS static route download.
	tacacs+	TACACS+ static route download.

### aaa group-configuration

To associate an authorization, authentication, and accounting (AAA) server group with an interface or customer profile, use the **aaa group-configuration** command in interface or customer profile configuration mode. To disable the configuration, use the **no** form of this command.

```
aaa group-configuration aaa-group-name
```

```
no aaa group-configuration aaa-group-name
```

Syntax Description	aaa-group-name	Character string used to name the group of AAA servers.
--------------------	----------------	---

	aaa-group-name	Character string used to name the group of AAA servers.
--	----------------	---

## aaa route download

To enable the download static route feature and set the amount of time between downloads, use the **aaa route download** global configuration command. To disable this function, use the **no** form of this command.

```
aaa route download [time]
```

```
no aaa route download
```

---

<b>Syntax Description</b>	<i>time</i>	(Optional) Time between downloads, in minutes. The range is 1 to 1440 minutes.
---------------------------	-------------	--

---

## accept dialin

To configure L2TP Network Servers (LNSs) to accept tunneled PPP connections from an L2TP Access Concentrator (LAC) and create an accept-dialin virtual private dialup network (VPDN) subgroup, use the **accept dialin** VPDN group configuration command. To remove the accept-dialin subgroup from a VPDN group, use the **no** form of this command.

```
accept dialin
```

```
no accept dialin
```

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

## accept dialout

To accept requests to tunnel Layer 2 Tunneling Protocol (L2TP) dial-out calls and create an accept-dialout VPDN subgroup, use the **accept dialout** VPDN group configuration command. To remove the accept-dialout subgroup from the VPDN group, use the **no** form of this command.

```
accept dialout
```

```
no accept dialout
```

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

## arap callback

To enable an AppleTalk Remote Access (ARA) client to request a callback, use the **arap callback** global configuration command. To disable callback requests, use the **no** form of this command.

**arap callback**

**no arap callback**

---

**Syntax Description** This command has no arguments or keywords.

## async default routing

To enable the router to pass routing updates to other routers over the AUX port configured as an asynchronous interface, use the **async default routing** interface configuration command. To disable dynamic addressing, use the **no** form of this command.

**async default routing**

**no async default routing**

---

**Syntax Description** This command has no arguments or keywords.

## async dynamic address

To specify dynamic asynchronous addressing, use the **async dynamic address** interface configuration command. To disable dynamic addressing, use the **no** form of this command.

**async dynamic address**

**no async dynamic address**

---

**Syntax Description** This command has no arguments or keywords.

## async dynamic routing

To enable manually configured routing on an asynchronous interface, use the **async dynamic routing** interface configuration command. To disable routing protocols, use the **no** form of this command; static routing is still used.

**async dynamic routing**

**no async dynamic routing**

---

**Syntax Description** This command has no arguments or keywords.

## async mode dedicated

To place a line into dedicated asynchronous mode using Serial Line Internet Protocol (SLIP) or PPP encapsulation, use the **async mode dedicated** interface configuration command. To return the line to interactive mode, use the **no** form of this command.

**async mode dedicated**

**no async mode dedicated**

---

**Syntax Description** This command has no arguments or keywords.

## async mode interactive

To return a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the **slip** and **ppp EXEC** commands, use the **async mode interactive** interface configuration command. To prevent users from implementing Serial Line Internet Protocol (SLIP) and PPP at the EXEC level, use the **no** form of this command.

**async mode interactive**

**no async mode interactive**

---

**Syntax Description** This command has no arguments or keywords.

## authen before-forward

To specify that the virtual private dialup network (VPDN) send the entire structured username to the authentication, authorization, and accounting (AAA) server the first time the router contacts the AAA server, use the **authen before-forward** VPDN group configuration command. To send just the domain name or Dialed Number Identification Service (DNIS), use the **no** form of this command.

**authen before-forward**

**no authen before-forward**

---

**Syntax Description** This command has no arguments or keywords.

## autocommand

To configure the Cisco IOS software to automatically execute a command when a user connects to a particular line, use the **autocommand** line configuration command. To disable the automatic execution, use the **no** form of this command.

**autocommand** *command*

**no autocommand** *command*

---

**Syntax Description** *command* Any appropriate EXEC command, including the host name and any switches that occur with the EXEC command.

---

## autodetect encapsulation

To enable automatic detection of the encapsulation types operating over a point-to-point link to a specified serial or ISDN interface, use the **autodetect encapsulation** interface configuration command. To disable automatic dynamic detection of the encapsulation types on a link, use the **no** form of this command.

**autodetect encapsulation** {**lapb-ta** | **ppp** | **v120**}

**no autodetect encapsulation** {**lapb-ta** | **ppp** | **v120**}

---

**Syntax Description**

<b>lapb-ta</b>	Link Access Procedure, Balanced (LAPB) for an ISDN terminal adapter.
<b>ppp</b>	PPP encapsulation on the interface.
<b>v120</b>	V.120 encapsulation on B channels.

---

## autohangup

To configure automatic line disconnect, use the **autohangup** line configuration command. To disable automatic line disconnect, use the **no** form of this command.

**autohangup**

**no autohangup**

**Syntax Description** This command has no arguments or keywords.

## autoselect

To configure a line to start an Appletalk Remote Access (ARA), PPP, or Serial Line Internet Protocol (SLIP) session, use the **autoselect** line configuration command. To disable this function on a line, use the **no** form of this command.

**autoselect** { **arap** | **ppp** | **slip** | **during-login** | **timeout** *seconds* }

**no autoselect** [*timeout*]

### Syntax Description

<b>arap</b>	ARA session.
<b>ppp</b>	PPP session.
<b>slip</b>	SLIP session.
<b>during-login</b>	Displays the username and/or password prompt without the user pressing the Return key. After the user logs in, the autoselect function begins.
<b>timeout</b> <i>seconds</i>	Timeout period from 1 to 120 seconds for the autoselect process. This argument applies only when the <b>arap</b> , <b>ppp</b> , or <b>slip</b> keyword functions are enabled and has no effect when the <b>during-login</b> keyword function is enabled.

## backup

To configure an IP backup endpoint address, enter the **backup** VPDN group configuration command. To remove this function, use the **no** form of this command.

**backup ip** *ip-address* [*limit number* [*priority number*]]

**no backup ip** *ip-address* [*limit number* [*priority number*]]

Syntax Description		
<b>ip</b> <i>ip-address</i>		IP address of the HGW/LNS at the other end of the tunnel. This is the IP endpoint at the end of the tunnel, which is an HGW/LNS router.
<b>limit</b> <i>number</i>		(Optional) Limits sessions per backup. The limit can range from 0 to 32767. The default is no limit set.
<b>priority</b> <i>number</i>		(Optional) Priority level. Loadsharing is priority 1. Backup priority is between 2 and 32,767. The highest priority is 2, which is the first home gateway router to receive backup traffic. The lowest priority is 32,767. The priority group is used to support multiple levels of loadsharing and backup. The default is the lowest priority.

## backup delay

To define how much time should elapse before a secondary line status changes after a primary line status has changed, use the **backup delay** interface configuration command. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

**backup delay** {*enable-delay-period* | **never**} {*disable-delay-period* | **never**}

**no backup delay** {*enable-delay-period* | **never**} {*disable-delay-period* | **never**}

Syntax Description		
<i>enable-delay-period</i>		Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.
<i>disable-delay-period</i>		Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.
<b>never</b>		Secondary line is never activated or deactivated.

## backup interface

To configure an interface as a secondary or dial backup, use the **backup interface** interface configuration command. To disable this feature, use the **no** form of this command.

### Cisco 7200 Series and Cisco 7500 Series Routers Only

**backup interface** *slot/port-adapter/port*

**no backup interface** *slot/port-adapter/port*

### Other Cisco Routers

**backup interface** *interface-type interface-number*

**no backup interface** *interface-type interface-number*

<b>Syntax Description</b>	<i>slotport-adapter/port</i>	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.
	<i>interface-type</i>	Interface type and port number to use as the backup interface.
	<i>interface-number</i>	

## backup interface dialer

To configure a dialer interface as a secondary or dial backup, use the **backup interface dialer** interface configuration command. To disable this feature, use the **no** form of this command.

**backup interface dialer** *number*

**no backup interface dialer** *number*

<b>Syntax Description</b>	<i>number</i>	Dialer interface number to use as the backup interface.
---------------------------	---------------	---

## backup load

To set a traffic load threshold for dial backup service, use the **backup load** interface configuration command. To return to the default value, use the **no** form of this command.

**backup load** {*enable-threshold* | **never**} {*disable-load* | **never**}

**no backup load** {*enable-threshold* | **never**} {*disable-load* | **never**}

<b>Syntax Description</b>	<i>enable-threshold</i>	Percentage of the primary line's available bandwidth that the traffic load must exceed to enable dial backup.
	<i>disable-load</i>	Percentage of the primary line's available bandwidth that the traffic load must be less than to disable dial backup.
	<b>never</b>	The secondary line is never activated due to traffic load.

## busyout

To inform a central-office switch that a channel is out-of-service, and to busyout an entire card on a dial shelf and remove it from dial services, use the **busyout** privileged EXEC command. To cancel busyout, use the **no** form of this command.

**busyout** *shelfslot/port*

**no busyout** *shelfslot/port*

<b>Syntax Description</b>	<i>shelfslot/port</i>	Shelf number, slot number, and port number. You must type in the forward slashes (/).
---------------------------	-----------------------	---

## busyout (port)

To disable a port by waiting for the active services on the specified port to terminate, use the **busyout** port configuration command. To re-enable the ports, use the **no** form of this command.

**busyout**

**no busyout**

---

**Syntax Description** This command has no arguments or keywords.

## busyout (spe)

To disable active calls on the specified Service Processing Elements (SPEs), use the **busyout** SPE configuration command. To re-enable the SPEs, use the **no** form of this command.

**busyout**

**no busyout**

---

**Syntax Description** This command has no arguments or keywords.

## call progress tone country

To specify the country code for retrieving the call progress tone parameters from the call progress tone database, use the **call progress tone country** global configuration command. To cancel the previous setting and to generate the call progress tones according to modem settings, use the **no** version of this command.

**call progress tone country** *country-name*

**no call progress tone country** *country-name*

---

<b>Syntax Description</b>	<i>country-name</i>	Selects default call progress tones (ring and cadence settings) for the specified country. Valid entries are: <b>argentina, australia, austria, belgium, brazil, canada, china, colombia, cyprus, czech-republic, denmark, finland, france, germany, greece, hongkong, hungary, iceland, india, indonesia, ireland, israel, italy, japan, korea, luxembourg, malaysia, mexico, netherlands, peru, philippines, poland, portugal, russia, singapore, slovakia, slovenia, south-africa, spain, sweden, switzerland, taiwan, thailand, turkey, unitedkingdom, usa, and venezuela.</b>
---------------------------	---------------------	--

---

## callback forced-wait

To force the Cisco IOS software to wait before initiating a callback to a requesting client, use the **callback forced-wait** global configuration command. To disable the forced waiting period, use the **no** form of this command.

**callback forced-wait**

**no callback forced-wait**

**Syntax Description** This command has no arguments or keywords.

## called-number

To assign a called party number to a pool of modems, use the **called-number** modem pool configuration command. To remove a number from a modem pool, use the **no** form of this command.

**called-number** *number* [**max-conn** *number*]

**no called-number** *number* [**max-conn** *number*]

<b>Syntax Description</b>	<i>number</i>	Called number for a modem pool.
	<b>max-conn</b> <i>number</i>	(Optional) Maximum number of simultaneous connections allowed for the called party number.

## calltracker call-record

To enable call record SYSLOG generation for the purpose of debugging, monitoring, or externally saving detailed call record information, use the **calltracker call-record** global configuration command. To disable call record SYSLOG generation, use the **no** form of this command.

**calltracker call-record** {**terse** | **verbose**} [**quiet**]

**no calltracker call-record** {**terse** | **verbose**} [**quiet**]

<b>Syntax Description</b>	<b>terse</b>	Generates a brief set of call records containing a subset of the data stored within Call Tracker used primarily to manage calls.
	<b>verbose</b>	Generates a complete set of call-records containing all of the data stored within Call Tracker used primarily to debug calls.
	<b>quiet</b>	(Optional) Call Record will be sent only to configured SYSLOG server and not to console.

## calltracker enable

To enable Call Tracker on the access server, use the **calltracker enable** global configuration command. To restore the default condition, use the **no** form of this command.

**calltracker enable**

**no calltracker enable**

---

**Syntax Description** This command has no arguments or keywords.

## calltracker history max-size

To set the maximum number of call entries stored in the Call Tracker history table, use the **calltracker history max-size** global configuration command. To restore the default value, use the **no** form of this command.

**calltracker history max-size** *number*

**no calltracker history max-size** *number*

---

**Syntax Description** *number* Maximum call entries to store in the Call Tracker history table. The valid range is from 0 through 10 times the maximum DS0 supported on a platform. A value of 0 prevents any history from being saved.

---

## calltracker history retain-mins

To set the number of minutes for which call entries are stored in the Call Tracker history table, use the **calltracker history retain-mins** global configuration command. To restore the default value, use the **no** form of this command.

**calltracker history retain-mins** *minutes*

**no calltracker history retain-mins** *minutes*

---

**Syntax Description** *minutes* The length of time to store calls in the Call Tracker history table. The valid range is from 0 through 26,000 minutes. A value of 0 prevents any history from being saved.

---

## call-type

To reject particular types of calls, use the **call-type** call discriminator profile configuration command. To disable this feature, use the **no** form of this command.

```
call-type { all | digital | speech | v110 | v120 }
```

```
no call-type { all | digital | speech | v110 | v120 }
```

Syntax Description	all	All calls.
	<b>digital</b>	Digital calls.
	<b>speech</b>	Speech calls.
	<b>v110</b>	V.110 calls.
	<b>v120</b>	V.120 calls.

## call-type cas

To statically set the call-type override for incoming channel-associated signalling (CAS) calls, use the **call-type cas** DNIS group configuration command. To disable this service, use the **no** form of this command.

```
call-type cas { digital | speech }
```

```
no call-type cas { digital | speech }
```

Syntax Description	digital	Override call type to digital. The incoming call with the DNIS in the called group is treated as a digital call type.
	<b>speech</b>	Override call-type to speech. The incoming call with the DNIS in the called group is treated as a speech call type.

## cas-custom

To customize signalling parameters for a particular E1 or T1 channel group on a channelized line, use the **cas-custom** controller configuration command. To disable the signalling customization, use the **no** form of this command.

```
cas-custom channel
```

```
no cas-custom channel
```

Syntax Description	<i>channel</i>	For E1, specifies a single channel group number, which can be from 0 to 30. This channel group number must match the channel number specified in the <b>cas-group</b> command.  For T1, specifies a single channel group number, which can be between 0 and 23.
--------------------	----------------	---

## cas-group (E1 controller)

To configure channel-associated signalling (CAS) on an E1 controller, use the **cas-group** controller configuration command. To disable CAS for one or more time slots, use the **no** form of this command.

**cas-group** *channel timeslots range type signal*

**no cas-group** *channel timeslots range type signal*

Syntax Description	
<i>channel</i>	Single channel group number from 0 to 30.
<b>timeslots</b> <i>range</i>	Time slot or time slot range, which can be from 1 to 31. You can specify a time slot range (for example, 1-29), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). The 16th time slot is reserved for out-of-band signalling.
<b>type</b> <i>signal</i>	<p>Type of CAS. Configure the signal type that your central office uses.</p> <p>For Cisco 5800 series access servers, replace the <i>signal</i> keyword with one of the following signal types:</p> <ul style="list-style-type: none"> <li>• <b>e&amp;m-fgb</b> [<b>dtmf</b> [<b>dnis</b>]   <b>mf</b> [<b>dnis</b>]]—Specifies ear and mouth channel signalling with feature group B support, which includes the wink start protocol. The optional signal tones are DTMF and MF with the option of provisioning DNIS.</li> <li>• <b>e&amp;m-fgd</b>—Specifies ear and mouth channel signalling with feature group D support, which includes the wink start protocol.</li> <li>• <b>e&amp;m-immediate-start</b>—Specifies ear and mouth channel signalling with immediate start support.</li> <li>• <b>fxs-ground-start</b>—Specifies Foreign Exchange Station ground start signalling support.</li> <li>• <b>fxs-loop-start</b>—Specifies Foreign Exchange Station loopstart signalling support.</li> <li>• <b>p7</b>—Specifies the P7 switch type.</li> <li>• <b>r2-analog</b> [<b>dtmf</b>   <b>r2-compelled</b> [<b>ani</b>]   <b>r2-non-compelled</b> [<b>ani</b>]   <b>r2-semi-compelled</b> [<b>ani</b>]]</li> <li>• <b>r2-digital</b> [<b>dtmf</b>   <b>r2-compelled</b> [<b>ani</b>]   <b>r2-non-compelled</b> [<b>ani</b>]   <b>r2-semi-compelled</b> [<b>ani</b>]]</li> <li>• <b>r2-pulse</b> [<b>dtmf</b>   <b>r2-compelled</b> [<b>ani</b>]   <b>r2-non-compelled</b> [<b>ani</b>]   <b>r2-semi-compelled</b> [<b>ani</b>]]</li> <li>• <b>sas-ground-start</b>—Specifies Special Access Station ground start signalling support.</li> <li>• <b>sas-loop-start</b>—Specifies Special Access Station loopstart signalling support.</li> </ul>

---

<b>type</b> <i>signal</i> (continued)	<p>For the Cisco 3600 series access servers, replace the <i>signal</i> variable with one of the following signal types:</p> <ul style="list-style-type: none"> <li>• <b>r2-analog</b> {<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]}</li> <li>• <b>r2-digital</b> {<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]}</li> <li>• <b>r2-pulse</b> {<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]}</li> </ul> <p>The following descriptions are provided for the previous R2 syntax bullets:</p> <p><b>r2-analog</b>—Specifies R2 ITU Q411 analog line signalling, which reflects the on/off switching of a tone in frequency-division multiplexing circuits (before TDM circuits were created). The tone is used for line signalling.</p> <p><b>r2-digital</b>—Specifies R2 ITU Q421 digital line signalling, which is the most common signalling configuration. The A and B bits are used for line signalling.</p> <p><b>r2-pulse</b>—Specifies R2 ITU supplement 7 pulse line signalling, which is a transmitted pulse that indicates a change in the line state.</p> <p><b>dtmf</b>—Specifies the DTMF tone signalling (Cisco 5800 series access server only).</p> <p><b>r2-compelled</b> [ani]—Specifies R2 compelled register signalling. You can also specify provisioning the ANI address option.</p> <p><b>r2-non-compelled</b> [ani]—Specifies R2 noncompelled register signalling.</p> <p><b>r2-semi-compelled</b> [ani]—Specifies R2 semicompelled register signalling.</p>
--	---

---

## cas-group (T1 controller)

To configure channelized T1 time slots with robbed-bit signalling, and R1 channel-associated signalling, use the **cas-group** controller configuration command. To disable signalling for one or more time slots, use the **no** form of this command.

### Cisco AS5200, Cisco AS5300, and Cisco AS5800 Series Access Servers

**cas-group** *channel* **timeslots** *range* **type** *signal*

**no cas-group** *channel* **timeslots** *range* **type** *signal*

### R1 Channel-Associated Signalling

**cas-group** *channel* **timeslots** *range* **type** **r1-modified** {**ani-dnis** | **dnis**}

**no cas-group** *channel* **timeslots** *range* **type** **r1-modified** {**ani-dnis** | **dnis**}

**Syntax Description**

<i>channel</i>	Single channel group number from 0 to 30.
<b>timeslots</b> <i>range</i>	Time slot or time slot range, which can be from 1 to 24 for T1, and from 1 to 31 for E1. You can specify a time slot range (for example, 1-31), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-7, 8, 17-31). The 16th time slot is reserved for out-of-band signalling.
<b>type</b> <i>signal</i>	Type of robbed-bit signalling. Replace the <i>signal</i> variable with one of the following signal types. The keywords <b>service</b> , <b>data</b> , and <b>voice</b> are used for switched 56K configuration. These keywords are described at the end of this syntax description table. <ul style="list-style-type: none"> <li>• <b>e&amp;m-fgb</b> [<b>dtmf</b> [<b>dnis</b>]   [<b>service</b> {<b>data</b>   <b>voice</b>}]   [<b>service</b> {<b>data</b>   <b>voice</b>}]   [<b>mf</b> [<b>dnis</b>]   [<b>service</b> {<b>data</b>   <b>voice</b>}]—Specifies ear and mouth channel signalling with feature group B support, which includes the wink start protocol. Use the options <b>dtmf</b> [<b>dnis</b>] to configure DTMF tone signalling with optional DNIS provisioning. Use the options <b>mf</b> [<b>dnis</b>] to configure MF tone signalling with optional DNIS provisioning. Use the options <b>service</b> {<b>data</b>   <b>voice</b>} for switched 56K configurations. (See the end of this syntax description table for more information about these switched 56K keywords.)</li> <li>• <b>e&amp;m-fgd</b> [<b>service</b> {<b>data</b>   <b>voice</b>}]—Specifies ear and mouth channel signalling with feature group D support, which includes the wink start protocol. Use the options <b>service</b> {<b>data</b>   <b>voice</b>} for switched 56K configurations. (See the end of this syntax description table for more information.)</li> <li>• <b>e&amp;m-immediate-start</b> [<b>service</b> {<b>data</b>   <b>voice</b>}]—Specifies ear and mouth channel signalling with immediate start support. Use the options <b>service</b> {<b>data</b>   <b>voice</b>} for switched 56K configurations. (See the end of this syntax description table for more information.)</li> <li>• <b>fxs-ground-start</b> [<b>service</b> {<b>data</b>   <b>voice</b>}]—Specifies Foreign Exchange Station ground start signalling support. Use the options [<b>service</b> {<b>data</b>   <b>voice</b>} for switched 56K configurations. (See the end of this syntax description table for more information.)</li> </ul>

**type** *signal*  
(continued)

- **fxs-loop-start** [**service** {**data** | **voice**}]—Specifies Foreign Exchange Station loopstart signalling support. Use the options **service** {**data** | **voice**} for switched 56K configurations. (See the end of this syntax description table for more information.)
- **r1-modified ani-dnis**—Indicates R1 signalling will collect ani and dnis information.
- **r1-modified dnis**—Indicates R1 signalling will collect only dnis information.
- **sas-ground-start** [**service** {**data** | **voice**}]—Specifies Special Access Station ground start signalling support. Use the options **service** {**data** | **voice**} for switched 56K configurations. (See the end of this syntax description table for more information.)
- **sas-loop-start** [**service** {**data** | **voice**}]—Specifies Special Access Station loopstart signalling support. Use the options **service** {**data** | **voice**} for switched 56K configurations.
- **service**—(Optional) Specifies the type of services provided for scenarios involving switched 56K connections. Do not include this option in the **cas-group** command statement if you are not using the access server to provide switched 56K connections.
- **data**—Enables switched 56K digital data services on the specified range of time slots. The data is directly read from the time slot or channel. Time slots configured with this option will not accept analog modem calls.
- **voice**—Enables analog modem services on the specified range of time slots. The call is forwarded to the modems for demodulation. Time slots configured with this option will not accept switched 56K digital calls.

## channel-group

To define the time slots that belong to each T1 or E1 circuit, use the **channel-group** controller configuration command. To clear the time slots for the T1 or E1 circuit, use the **no** form of this command.

**channel-group** *channel-number* **timeslots** *range* [**speed** {**48** | **56** | **64**}]

**no channel-group** [*channel-number* **timeslots** *range*]

### Syntax Description

<i>channel-number</i>	Channel-group number. When configuring a T1 data line, channel-group numbers can be values from 0 to 23. When configuring an E1 data line, channel-group numbers can be values from 0 to 30.
<b>timeslots</b> <i>range</i>	One or more time slots or ranges of time slots belonging to the channel group. The first time slot is numbered 1. For a T1 controller, the time slot range is from 1 to 24. For an E1 controller, the time slot range is from 1 to 31.
<b>speed</b> { <b>48</b>   <b>56</b>   <b>64</b> }	(Optional) Speed of the underlying DS0s. See the Usage Guidelines section for additional information.

## chat-script

To create a script that will place a call over a modem, use the **chat-script** global configuration command. To disable the specified chat script, use the **no** form of this command.

**chat-script** *script-name expect-send*

**no chat-script** *script-name expect-send*

### Syntax Description

<i>script-name</i>	Name of the chat script.
<i>expect-send</i>	Pairs of information elements: an item to expect and an item to send in response.

## class

To create a signaling class structure that can be referred to by its name, use the **class** controller configuration command. To remove the structure, use the **no** form of this command.

**class** *name*

**no class** *name*

### Syntax Description

<i>name</i>	The signalling class name which specifies the template that processes the ANI/DNIS delimiter.
-------------	---

## clear controller

To reset the T1 or E1 controller, use the **clear controller** EXEC command.

### Cisco 7200 Series and Cisco 7500 Series Routers

**clear controller** {**t1** | **e1**} *slot/port*

### Cisco AS5200 Series and Cisco AS5300 Series Routers

**clear controller** {**t1** | **e1**} *number*

### Syntax Description

<b>t1</b>	T1 controller.
<b>e1</b>	E1 controller.
<i>slot/port</i>	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.
<i>number</i>	Network interface module (NIM) number, in the range 0 through 2.

## clear cot summary

To reset the counters, use the **clear cot summary** privileged EXEC command.

```
clear cot summary
```

---

**Syntax Description** This command has no arguments or keywords.

## clear counters (async)

To clear the counters of a specified asynchronous interface or specified asynchronous interface group, as displayed by the **show interface async** command, use the **clear counters** EXEC command.

```
clear counters {async async-interface-number | group-async group-async-interface-number}
```

---

<b>Syntax Description</b>	<b>async</b>	Counters in a specified asynchronous interface.
	<i>async-interface-number</i>	Required async interface number of the asynchronous interface that has been previously created with this number specification. The range is from 1 through 49.
	<b>group-async</b>	Counters in a specified asynchronous interface group.
	<i>group-async-interface-number</i>	Required group-async interface number that has been previously created with this number specification. The range is from 0 through 49.

---

## clear counters line

To clear line counters, use the **clear counters line** EXEC command.

```
clear counters line {type | number}
```

---

<b>Syntax Description</b>	<i>type</i>	Line type: <b>aux</b> , <b>console</b> , <b>tty</b> , or <b>vty</b> .
	<i>number</i>	First line number to clear, which can be between 0 and 54.

---

## clear dialer

To clear the values of dialer statistics for one or more serial interfaces or BRIs configured for dial-on-demand routing (DDR), use the **clear dialer** privileged EXEC mode command.

```
clear dialer [interface interface-type interface-number]
```

**Cisco 7500 Series Routers Only**

```
clear dialer [interface serial slot/port]
```

Syntax Description		
	<b>interface</b>	(Optional) Indicates that one interface will be specified.
	<i>interface-type</i>	(Optional) Interface type: <b>async</b> , <b>serial</b> , or <b>bri</b> .
	<i>interface-number</i>	(Optional) Interface number.
	<i>slot/port</i>	(Optional) Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.

## clear dialer dnis

To reset the counter statistics associated with a specific dialed number identification service (DNIS) group or number, use the **clear dialer dnis** privileged EXEC command.

```
clear dialer dnis {group name | number number}
```

Syntax Description		
	<b>group <i>name</i></b>	Dialer DNIS group statistics.
	<b>number <i>number</i></b>	Dialer DNIS number statistics.

## clear dialer sessions

To remove all dialer sessions and disconnect links when connected, use the **clear dialer sessions** EXEC command.

```
clear dialer sessions
```

Syntax Description	
	This command has no arguments or keywords.

## clear dsip tracing

To clear Distributed System Interconnect Protocol (DSIP) tracing statistics (trace logging), use the **clear dsip tracing** privileged EXEC command.

```
clear dsip tracing {counters | tracing} [control | data | ipc]
```

Syntax Description		
	<b>counters</b>	DSIP counters.
	<b>tracing</b>	DSIP tracing buffers.
	<b>control</b>	(Optional) Control counters or tracing buffers.
	<b>data</b>	(Optional) Data counters or tracing buffers.
	<b>ipc</b>	(Optional) Inter-process communication counters or tracing buffers.

## clear interface

To reset the hardware logic on an interface, use the **clear interface** privileged EXEC command.

```
clear interface name-tag
```

Syntax Description	<i>name-tag</i>	Name to identify the server configuration so that multiple entries of server configuration can be entered.
--------------------	-----------------	--

## clear interface virtual-access

To tear down the virtual access interface and free the memory for other dial-in uses, use the **clear interface virtual-access** EXEC command.

```
clear interface virtual-access number
```

Syntax Description	<i>number</i>	Virtual access interface number.
--------------------	---------------	----------------------------------

## clear ip route download

To clear static routes downloaded from an authentication, authorization, and accounting (AAA) server, use the **clear ip route download** EXEC command.

```
clear ip route download { * | network-number network-mask | reload }
```

Syntax Description	*	All routes.
	<i>network-number</i>	Destination network route and mask in standard IP address notation. For example, 10.1.1.1 255.255.255.255.
	<i>network-mask</i>	
	<b>reload</b>	Delete all routes, then reload static routes from the AAA server and reset the timer configured by the <b>aaa route download</b> command.

## clear line

To return a terminal line to idle state, use the **clear line** EXEC command.

```
clear line line-number
```

Syntax Description	<i>line-number</i>	Absolute line number.
--------------------	--------------------	-----------------------

## clear line async-queue

To reset the connections currently waiting to use a rotary line in the queue, use the **clear line async-queue** EXEC command.

```
clear line async-queue [rotary-group]
```

Syntax Description	
	<i>rotary-group</i> (Optional) Rotary group.

## clear modem

To reset the hardware for one or more manageable modems on an access server or router, use the **clear modem** EXEC command.

```
clear modem {slot/port | all | group group-number | at-mode slot/port | test}
```

Syntax Description	
<i>slot/port</i>	Slot and modem port number. (Include the forward slash (/) when entering this variable. For example: <b>1/1</b> .)
<b>all</b>	All modems. This command disconnects any active calls.
<b>group</b> <i>group-number</i>	Group of modems. The modem group number is the number of the group you have previously created.
<b>at-mode</b> <i>slot/port</i>	AT directly connected session. The variable, <i>slot/port</i> , is required. This EXEC command clears an attention (AT) directly connected session to a manageable Microcom modem from a second Telnet session.
<b>test</b>	Log or test report that is displayed by the <b>show modem test</b> command. If you do not clear the test regularly, eventually the oldest test report will replace the current test report.

## clear modem counters

To clear the statistical counters on one or more manageable modems installed in an access server, use the **clear modem counters** EXEC command.

```
clear modem counters [slot/port-number | group [group-number]]
```

Syntax Description	
<i>slot/port-number</i>	(Optional) Slot and modem port number. (Include the forward slash (/) when entering this variable. For example: <b>1/1</b> .)
<b>group</b> [ <i>group-number</i> ]	(Optional) One or all groups of modems. The optional modem group number is the number of a group-async interface. The group number range is 1 through 1002.

## clear modempool-counters

To clear the active or running counters associated with one or more modem pools, use the **clear modempool-counters EXEC** command.

```
clear modempool-counters [name]
```

Syntax Description	
	<i>name</i> (Optional) Modem pool name. If you do not include this option, all counters for all modem pools will be cleared.

## clear port

To reset the NextPort port and clear any active call to the port, use the **clear port EXEC** command.

### Cisco AS5400 with NextPort DFC

```
clear port [slot | slot/port]
```

### Cisco AS5800 with Universal Port Card

```
clear port [shelfslot | shelfslot/port]
```

Syntax Description	
<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/port</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
<i>shelfslot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
<i>shelfslot/port</i>	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

## clear port log

To clear all event entries in the port level history event log, use the **clear port log EXEC** command.

### Cisco AS5400 with NextPort DFC

```
clear port log [slot | slot/port]
```

### Cisco AS5800 with Universal Port Card

```
clear port log [shelfslot | shelfslot/port]
```

Syntax Description		
	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/port</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
	<i>shelf/slot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/port</i>	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

## clear resource-pool

To reset the counter statistics associated with a specific customer profile, call discriminator, or physical resource, use the **clear resource-pool** privileged EXEC command.

```
clear resource-pool {customer | discriminator | resource} {name | all}
```

Syntax Description		
	<b>customer</b>	Customer profile.
	<b>discriminator</b>	Call discriminator.
	<b>resource</b>	Physical resource. Checks the counters maintained for resource groups.
	<i>name</i>	Specific customer profile, discriminator, or physical resource in the access server.
	<b>all</b>	All customer profiles, discriminators, or physical resources in the access server.

## clear rlm group link

To clear all time stamps to zero, use the **clear rlm group link** privileged EXEC command.

```
clear rlm group group-number link
```

Syntax Description		
	<i>group-number</i>	RLM group number (0 to 255).

## clear snapshot quiet-time

To end the quiet period on a client router within 2 minutes, use the **clear snapshot quiet-time** EXEC command.

```
clear snapshot quiet-time interface-type interface-number
```

Syntax Description		
	<i>interface-type</i>	Interface type and number.
	<i>interface-number</i>	

## clear spe

To reboot all specified Service Processing Elements (SPEs), use the **clear spe** EXEC command.

### Cisco AS5400 with NextPort DFC

```
clear spe [slot | slot/spe]
```

### Cisco AS5800 with Universal Port Card

```
clear spe [shelf/slot | shelf/slot/spe]
```

Syntax Description	slot	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	slot/spe	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	shelf/slot	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	shelf/slot/spe	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## clear spe counters

To clear all statistics, use the **clear spe counters** EXEC command.

### Cisco AS5400 with NextPort DFC

```
clear spe counters [slot | slot/spe]
```

### Cisco AS5800 with Universal Port Card

```
clear spe counters [shelf/slot | shelf/slot/spe]
```

Syntax Description	slot	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	slot/spe	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	shelf/slot	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	shelf/slot/spe	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## clear spe log

To clear event entries in the slot history event log, use the **clear spe log** EXEC command.

### Cisco AS5400 with NextPort DFC

```
clear spe log [slot]
```

### Cisco AS5800 with Universal Port Card

```
clear spe log [shelf/slot]
```

Syntax Description		
	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>shelf/slot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.

## clear vpdn history failure

To clear the content of the failure history table, use the **clear vpdn history failure** EXEC command.

```
clear vpdn history failure
```

Syntax Description	
	This command has no arguments or keywords.

## clear vpdn tunnel

To shut down a specified tunnel and all sessions within the tunnel, use the **clear vpdn tunnel** EXEC command.

```
clear vpdn tunnel [pptp | l2f | l2tp] network-access-server gateway-name
```

Syntax Description		
	<b>pptp</b>	(Optional) Clears the specified Point-to-Point Tunneling Protocol (PPTP) tunnel.
	<b>l2f</b>	(Optional) Clears the specified Layer 2 Forwarding (L2F) tunnel.
	<b>l2tp</b>	(Optional) Clears the specified Layer 2 Tunneling Protocol (L2TP) tunnel.
	<i>network-access-server</i>	Name of the network access server at the far end of the tunnel, probably the point of presence of the public data network or the ISP.
	<i>gateway-name</i>	Host name of home gateway at the local end of the tunnel.

## clid group

To add a calling line identifier (CLID) group to a discriminator, use the **clid group** CLID configuration command. To remove a CLID group from a discriminator, use the **no** form of this command.

**clid group** { *clid-group-name* | **default** }

**no clid group** { *clid-group-name* | **default** }

Syntax Description		
	<i>clid-group-name</i>	Name of the CLID group added to the discriminator. You can add an existing CLID group or one that is to be defined. Discrimination does not happen until the CLID group is defined.
	<b>default</b>	Default discrimination profile. Any CLID number coming in on a call is in its respective default group unless it is specifically assigned a CLID group name.

## clock source line

To set the E1 line clock source for the Cisco AS5200 access server, use the **clock source line** controller configuration command. To change or remove the clocking source, use the **no** form of this command.

**clock source line** { **primary** | **secondary** }

**no clock source line** { **primary** | **secondary** }

Syntax Description		
	<b>primary</b>	Primary TDM clock source.
	<b>secondary</b>	Secondary TDM clock source.

## controller

To configure a T1 or E1 controller and enter controller configuration mode, use the **controller** global configuration command.

### Cisco 7200 Series and Cisco 7500 Series Routers

**controller** { **t1** | **e1** } *slot/port*

### Cisco AS5200 and AS5300 Access Servers and Cisco 4000 Series Routers

**controller** { **t1** | **e1** } *number*

Syntax Description		
	<b>t1</b>	T1 controller.
	<b>e1</b>	E1 controller.

<i>slot/port</i>	Backplane slot number and port number on the interface. See your hardware installation manual for the specific values and slot numbers.
<i>number</i>	Network processor module (NPM) number, in the range 0 through 2.

## copy modem

To copy modem firmware to integrated modems in an access server, use the **copy modem EXEC** command.

```
copy {flash | tftp | rcp} modem
```

Syntax Description	flash	Flash memory.
	tftp	Local TFTP server.
	rcp	Local rcp server.

## corlist incoming

To specify the class of restrictions (COR) list to be used when a specified dial peer acts as the incoming dial peer, use the **corlist incoming** dial-peer configuration command. To clear the previously defined incoming COR list in preparation for redefining the incoming COR list, use the **no** form of this command.

```
corlist incoming cor-list-name
```

```
no corlist incoming cor-list-name
```

Syntax Description	<i>cor-list-name</i>	Name of the dial peer COR list that defines the capabilities that the specified dial peer has when it is used as an incoming dial peer.
--------------------	----------------------	---

## corlist outgoing

To specify the class of restrictions (COR) list to be used by outgoing dial peers, use the **corlist outgoing** dial-peer configuration command. To clear the previously defined outgoing COR list in preparation for redefining the outgoing COR list, use the **no** form of this command.

```
corlist outgoing cor-list-name
```

```
no corlist outgoing cor-list-name
```

Syntax Description	<i>cor-list-name</i>	Required name of the dial peer COR list for outgoing calls to the configured number using this dial peer.
--------------------	----------------------	---

## cpp authentication

To enable negotiation of authentication with a router or bridge that supports the Combinet Proprietary Protocol (CPP) and that is calling in to this router, use the **cpp authentication** interface configuration command. To disable negotiation of CPP authentication, use the **no** form of this command.

**cpp authentication**

**no cpp authentication**

**Syntax Description** This command has no arguments or keywords.

## cpp callback accept

To enable the router to accept callback from a router or bridge that supports the Combinet Proprietary Protocol (CPP), use the **cpp callback accept** interface configuration command. To disable callback acceptance, use the **no** form of this command.

**cpp callback accept**

**no cpp callback accept**

**Syntax Description** This command has no arguments or keywords.

## default (VPDN)

To reset a virtual private dialup network (VPDN) group or a VPDN subgroup to its default value, use the **default** VPDN group or VPDN subgroup command.

**default** { **accept-dialin** | **accept-dialout** | **authen before-forward** | **dialer** | **dnis** | **domain** | **force-local-chap** | **initiate-to** | **l2f** | **l2tp** | **lcp renegotiation** | **local** | **multilink** | **pool-member** | **request-dialin** | **request-dialout** | **rotary-group** | **source-ip** | **terminate-from** | **virtual-template** }

### Syntax Description

<b>accept-dialin</b>	Removes the <b>accept-dialin</b> group from the VPDN group.
<b>accept-dialout</b>	Removes the <b>accept-dialout</b> group from the VPDN group.
<b>authen before-forward</b>	Removes the <b>authen before-forward</b> command from the VPDN group.
<b>dialer</b>	Removes the <b>dialer</b> command from the <b>accept-dialout</b> group.
<b>dnis</b>	Removes all <b>dnis</b> commands from the <b>request-dialin</b> group.
<b>domain</b>	Removes all <b>domain</b> commands from the <b>request-dialin</b> group.
<b>force-local-chap</b>	Removes the <b>force-local-chap</b> command from the VPDN group.
<b>initiate-to</b>	Removes all <b>initiate-to</b> commands from the VPDN group.

<b>l2f</b>	Removes all <b>l2f</b> commands from the VPDN group.
<b>l2tp</b>	Removes all <b>l2tp</b> commands from the VPDN group.
<b>lcp renegotiation</b>	Removes the <b>lcp renegotiation</b> command from the VPDN group.
<b>local</b>	Removes the <b>local</b> command from the VPDN group.
<b>multilink</b>	Removes all <b>multilink</b> commands from the VPDN group.
<b>pool-member</b>	Removes the <b>pool-member</b> command from the request-dialout group.
<b>request-dialin</b>	Removes the request-dialin group from the VPDN group.
<b>request-dialout</b>	Removes the request-dialout group from the VPDN group.
<b>rotary-group</b>	Removes the <b>rotary-group</b> command from the request-dialout group.
<b>source-ip</b>	Removes the <b>source-ip</b> command from the VPDN group.
<b>terminate-from</b>	Removes the <b>terminate-from</b> command from the VPDN group.
<b>virtual-template</b>	Removes the <b>virtual-template</b> command from the accept-dialin group.

## description

To add a description to an interface configuration, use the **description** interface configuration command. To remove the description, use the **no** form of this command.

**description** *string*

**no description**

### Syntax Description

*string* Comment or a description to help you remember what is attached to this interface.

## description (vpdn-group)

To add a description to a VPDN group, use the **description** VPDN group configuration command. To remove the description, use the **no** form of this command.

**description** *string*

**no description**

### Syntax Description

*string* Comment or a description about the VPDN group.

## dialer

To specify the dialer interface that an accept-dialout virtual private dialup network (VPDN) subgroup will use to dial out calls, use the **dialer** accept-dialout configuration command. To remove the dialer interface from the accept-dialout VPDN subgroup, use the **no** form of this command.

**dialer** *dialer-interface*

**no dialer**

Syntax Description	
	<i>dialer-interface</i> Number of the dialer interface.

## dialer callback-secure

To enable callback security, use the **dialer callback-secure** interface configuration command. To disable callback security, use the **no** form of this command.

**dialer callback-secure**

**no dialer callback-secure**

Syntax Description	
	This command has no arguments or keywords.

## dialer callback-server

To enable an interface to make return calls when callback is successfully negotiated, use the **dialer callback-server** interface configuration command. To disable return calls, use the **no** form of this command.

**dialer callback-server** [**username dialstring**]

**no dialer callback-server**

Syntax Description	
<b>username</b>	(Optional) Looks up the authenticated host name in a <b>dialer map</b> command. This is the default.
<b>dialstring</b>	(Optional) Identifies the return call during callback negotiation.

## dialer called

To configure dial-on-demand routing (DDR) to perform DNIS-plus-ISDN-subaddress binding for dialer profile interfaces, use the **dialer called** dial-on-demand routing configuration command. To disable DNIS-plus-ISDN-subaddress binding, use the **no** form of this command.

**dialer called** *DNIS:subaddress*

**no dialer called** *DNIS:subaddress*

---

### Syntax Description

*DNIS:subaddress* Dialed Number Identification Service or the called party number, a colon, and the ISDN subaddress.

---

## dialer caller

To configure caller ID screening and optionally to enable ISDN caller ID callback for legacy dial-on-demand routing (DDR) or the dialer profiles DDR feature, use the **dialer caller** interface configuration command. To disable this feature, use the **no** form of this command.

**dialer caller** *number* [*callback*]

**no dialer caller** *number* [*callback*]

---

### Syntax Description

*number* Remote telephone number for which to screen. Use a letter X to represent a single “don’t care” digit. The maximum length of each number is 25 characters.

*callback* (Optional) Enables callback.

---

## dialer clid group

To create a Calling Line Identification (CLID) group in the resource pool and assign it a name, use the **dialer clid group** global configuration command. To remove a CLID group from the resource pool, use the **no** form of this command.

**dialer clid group** *clid-group-name*

**no dialer clid group** *clid-group-name*

---

### Syntax Description

*clid-group-name* Name of the CLID group created in the resource pool.

---

## dialer congestion-threshold

To specify congestion threshold in connected links, use the **dialer congestion-threshold** interface configuration command. To disable this function, use the **no** form of this command.

**dialer congestion-threshold** *links*

**no dialer congestion-threshold**

<b>Syntax Description</b>	<i>links</i>	Number of connected links for congestion threshold in the range 0 to 64,000.
---------------------------	--------------	--

## dialer dnis group

To create a DNIS group, use the **dialer dnis group** global configuration command. To remove a specific Dialed Number Identification Service (DNIS) group from the running configuration, use the **no** form of this command.

**dialer dnis group** *name*

**no dialer dnis group** *name*

<b>Syntax Description</b>	<i>name</i>	Name to assign to the DNIS group number.
---------------------------	-------------	--

## dialer dns

To obtain a user profile name on a remote network using reverse Domain Name System (DNS), use the **dialer dns** interface configuration command. To disable this function, use the **no** form of this command.

**dialer dns**

**no dialer dns**

<b>Syntax Description</b>	This command has no arguments or keywords.	
---------------------------	--	--

## dialer dtr

To enable dial-on-demand routing (DDR) on an interface and specify that the serial line is connected by non-V.25bis modems using Electronic Industries Association (EIA) signalling only—specifically, the data terminal ready (DTR) signal—use the **dialer dtr** interface configuration command. To disable DDR for the interface, use the **no** form of this command.

**dialer dtr**

**no dialer dtr**

---

**Syntax Description** This command has no arguments or keywords.

## dialer enable-timeout

To set the length of time an interface stays down after a call has completed or failed and before it is available to dial again, use the **dialer enable-timeout** interface configuration command. To return to the default value, use the **no** form of this command.

**dialer enable-timeout** *seconds*

**no dialer enable-timeout**

---

**Syntax Description** *seconds* Time, in seconds, that the Cisco IOS software waits before the next call can occur on the specific interface. Acceptable values are positive, nonzero integers.

This value must be greater than the serial pulse interval for this interface, set via the **pulse-time** command.

---

## dialer fast-idle (interface configuration)

To specify the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed, use the **dialer fast-idle** interface configuration command. To return to the default value, use the **no** form of this command.

**dialer fast-idle** *seconds*

**no dialer fast-idle**

---

**Syntax Description** *seconds* Idle time, in seconds, that must occur on an interface before the line is disconnected. Acceptable values are positive, nonzero integers.

---

## dialer fast-idle (map-class dialer configuration)

To specify the fast idle timer value to use when placing a call to any telephone number associated with a specified class, use the **dialer fast-idle** map-class dialer configuration command. To reset the dialer fast-idle timer to the default, use the **no** form of this command.

**dialer fast-idle** *seconds*

**no dialer fast-idle**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds to wait before placing a different call.
---------------------------	----------------	--

## dialer-group

To control access by configuring an interface to belong to a specific dialing group, use the **dialer-group** interface configuration command. To remove an interface from the specified dialer access group, use the **no** form of this command.

**dialer-group** *group-number*

**no dialer-group**

<b>Syntax Description</b>	<i>group-number</i>	Number of the dialer access group to which the specific interface belongs. This access group is defined with the <b>dialer-list</b> command. Acceptable values are nonzero, positive integers between 1 and 10.
---------------------------	---------------------	---

## dialer hold-queue

To allow *interesting* outgoing packets to be queued until a modem connection is established, use the **dialer hold-queue** interface configuration command. To disable the hold queue, use the **no** form of this command.

**dialer hold-queue** *packets timeout seconds*

**no dialer hold-queue** [*packets*]

<b>Syntax Description</b>	<i>packets</i>	Number of packets, in the range 1 to 100 packets, to hold in the queue. This argument is optional with the <b>no</b> form of this command.
	<b>timeout</b> <i>seconds</i>	Amount of time, in seconds, to queue the packets.

## dialer idle-timeout (interface)

To specify the duration of idle time before a line is disconnected, use the **dialer idle-timeout** interface configuration command. To reset the idle timeout to the default, use the **no** form of this command.

**dialer idle-timeout** *seconds* [**inbound** | **either**]

**no dialer idle-timeout**

<b>Syntax Description</b>	<i>seconds</i>	Idle time, in seconds, that must occur on the interface before the line is disconnected. Acceptable values are positive, nonzero integers.
	<b>inbound</b>	(Optional) Only inbound traffic will reset the idle timeout.
	<b>either</b>	(Optional) Both inbound and outbound traffic will reset the idle timeout.

## dialer in-band

To specify that dial-on-demand routing (DDR) is to be supported, use the **dialer in-band** interface configuration command. To disable DDR for the interface, use the **no** form of this command.

**dialer in-band** [**no-parity** | **odd-parity**]

**no dialer in-band**

<b>Syntax Description</b>	<b>no-parity</b>	(Optional) No parity is to be applied to the dialer string that is sent out to the modem on synchronous interfaces.
	<b>odd-parity</b>	(Optional) Dialed number has odd parity (7-bit ASCII characters with the eighth bit as the parity bit) on synchronous interfaces.

## dialer isdn

To specify the bit rate used on the B channel associated with a specified map class and to specify whether to set up semipermanent connections for this map class, use the **dialer isdn** map-class dialer configuration command. To remove the speed and connection settings, use the **no** form of this command.

**dialer isdn** [**speed** *speed*] [**spc**]

**no dialer isdn** [**speed** *speed*] [**spc**]

<b>Syntax Description</b>	<b>speed</b> <i>speed</i>	(Optional) Bit rate, in kilobytes per second (kbps), used on the ISDN B channel. Values are <b>56</b> and <b>64</b> . Defaults is 64.
	<b>spc</b>	(Optional) ISDN semipermanent connection is used for calls associated with this map class.

## dialer isdn short-hold

To configure the router to disconnect a call at the end of the current charging period if the line has been idle for at least the specified minimum period, use the **dialer isdn short-hold** map-class dialer configuration command. To reset the ISDN short-hold timer to the default period, use the **no** form of this command.

**dialer isdn short-hold** *seconds*

**no dialer isdn short-hold**

Syntax Description	<i>seconds</i>	Minimum number of seconds of idle time on the line. Default is 120 seconds.
--------------------	----------------	---

## dialer-list protocol

To define a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list, use the **dialer-list protocol** global configuration command. To delete a dialer list, use the **no** form of this command.

**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}

**no dialer-list** *dialer-group* [**protocol** *protocol-name* [**list** *access-list-number* | *access-group*]]

Syntax Description	<i>dialer-group</i>	Number of a dialer access group identified in any <b>dialer-group</b> interface configuration command.
	<i>protocol-name</i>	One of the following protocol keywords: <b>appletalk</b> , <b>bridge</b> , <b>clns</b> , <b>clns_es</b> , <b>clns_is</b> , <b>decnet</b> , <b>decnet_router-L1</b> , <b>decnet_router-L2</b> , <b>decnet_node</b> , <b>ip</b> , <b>ipx</b> , <b>vines</b> , or <b>xns</b> .
	<b>permit</b>	Permits access to an entire protocol.
	<b>deny</b>	Denies access to an entire protocol.
	<b>list</b>	Specifies that an access list will be used for defining a granularity finer than an entire protocol.
	<i>access-list-number</i>	Access list numbers specified in any DECnet, Banyan VINES, IP, Novell IPX, or XNS standard or extended access lists, including Novell IPX extended service access point (SAP) access lists and bridging types. See Table 38 for the supported access list types and numbers.
	<i>access-group</i>	Filter list name used in the <b>clns filter-set</b> and <b>clns access-group</b> commands.

**Table 38** *dialer-list Command Supported Access List Types and Numbers*

Access List Type	Access List Number Range (Decimal)
AppleTalk	600–699
Banyan VINES (standard)	1–100

**Table 38** *dialer-list Command Supported Access List Types and Numbers (continued)*

Access List Type	Access List Number Range (Decimal)
Banyan VINES (extended)	101–200
DECnet	300–399
IP (standard)	1–99
IP (extended)	100–199
Novell IPX (standard)	800–899
Novell IPX (extended)	900–999
Transparent Bridging	200–299
XNS	500–599

## dialer load-threshold

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the **dialer load-threshold** interface configuration command. To disable the setting, use the **no** form of this command.

**dialer load-threshold** *load* [**outbound** | **inbound** | **either**]

**no dialer load-threshold**

### Syntax Description

<i>load</i>	Interface load used to determine whether to initiate another call or to drop a link to the destination. This argument represents a utilization percentage; it is a number between 1 and 255, where 255 is 100 percent.
<b>outbound</b>	(Optional) Calculates the actual load using outbound data only.
<b>inbound</b>	(Optional) Calculates the actual load using inbound data only.
<b>either</b>	(Optional) Sets the maximum calculated load as the larger of the outbound and inbound loads.

## dialer map

To configure a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites, use a form of the **dialer map** interface configuration command; all options are shown in the first form of this command. To delete a particular dialer map entry, use the **no** form of this command.

**dialer map** *protocol next-hop-address* [**name** *host-name*] [**spc**] [**speed 56** | **speed 64**] [**broadcast**] [**modem-script** *modem-regexp*] [**system-script** *system-regexp*] [*dial-string[:isdn-subaddress]*]

**no dialer map** *protocol next-hop-address* [**name** *host-name*] [**spc**] [**speed 56** | **speed 64**] [**broadcast**] [**modem-script** *modem-regexp*] [**system-script** *system-regexp*] [*dial-string[:isdn-subaddress]*]

To configure a serial interface or ISDN interface to place a call to multiple sites and to authenticate calls from multiple sites, use the second form of the **dialer map** command:

```
dialer map protocol next-hop-address [name host-name] [spc] [speed 56 | speed 64] [broadcast]
[dial-string[:isdn-subaddress]]
```

```
no dialer map protocol next-hop-address [name host-name] [spc] [speed 56 | speed 64]
[broadcast] [dial-string[:isdn-subaddress]]
```

To configure a serial interface or ISDN interface to support bridging, use the third form of this command:

```
dialer map bridge [name host-name] [spc] [broadcast] [dial-string[:isdn-subaddress]]
```

```
no dialer map bridge [name host-name] [spc] [broadcast] [dial-string[:isdn-subaddress]]
```

To configure an asynchronous interface to place a call to a single site that requires a system script or that has no assigned modem script, or to multiple sites on a single line, on multiple lines, or on a dialer rotary group, use the fourth form of the **dialer map** command:

```
dialer map protocol next-hop-address [name host-name] [broadcast] [modem-script
modem-regexp] [system-script system-regexp] [dial-string]
```

```
no dialer map protocol next-hop-address [name host-name] [broadcast] [modem-script
modem-regexp] [system-script system-regexp] [dial-string]
```

#### Syntax Description

<i>protocol</i>	Protocol keywords; one of the following: <b>appletalk</b> , <b>bridge</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , <b>ipx</b> , <b>novell</b> , <b>snapshot</b> , <b>vines</b> , and <b>xns</b> .
<i>next-hop-address</i>	Protocol address used to match against addresses to which packets are destined. This argument is not used with the <b>bridge</b> protocol keyword.
<b>name</b>	(Optional) The remote system with which the local router or access server communicates. Used for authenticating the remote system on incoming calls.
<i>host-name</i>	(Optional) Case-sensitive name or ID of the remote device (usually the host name). For routers with ISDN interfaces, if calling line identification—sometimes called CLI, but also known as caller ID and automatic number identification (ANI)—is provided, the <i>host-name</i> field can contain the number that the calling line ID provides.
<b>spc</b>	(Optional) Semipermanent connection between customer equipment and the exchange; used only in Germany for circuits between an ISDN BRI and a 1TR6 ISDN switch and in Australia for circuits between an ISDN PRI and a TS-014 switch.
<b>speed 56   speed 64</b>	(Optional) Keyword and value indicating the line speed in kilobits per second to use. Used for ISDN only. The default speed is <b>speed 64</b> (64 kbps).
<b>broadcast</b>	(Optional) Broadcasts should be forwarded to this protocol address.
<b>modem-script</b>	(Optional) A modem script is used for the connection (for asynchronous interfaces).
<i>modem-regexp</i>	(Optional) Regular expression to which a modem script will be matched (for asynchronous interfaces).

<b>system-script</b>	(Optional) A system script is used for the connection (for asynchronous interfaces).
<i>system-regexp</i>	(Optional) Regular expression to which a system script will be matched (for asynchronous interfaces).
<i>dial-string[:isdn-subaddress]</i>	(Optional) Telephone number sent to the dialing device when it recognizes packets with the specified next hop address that matches the access lists defined, and the optional subaddress number used for ISDN multipoint connections. The dial string and ISDN subaddress, if used, must be the last item in the command line.

## dialer map (AOC)

To configure an ISDN interface to place a call to multiple sites, to authenticate calls from multiple sites, and to identify the class name that configures the ISDN Advice of Charge (AOC) short-hold idle timeout, use the following form of the **dialer map** interface configuration command. To delete a particular dialer map entry, use the **no** form of this command.

```
dialer map protocol next-hop-address [name host-name] [spc] [speed 56 | speed 64] [broadcast]
class class-name [dial-string[:isdn-subaddress]]
```

```
no dialer map protocol next-hop-address [name host-name] [spc] [speed 56 | speed 64]
[broadcast] class class-name [dial-string[:isdn-subaddress]]
```

Syntax Description	
<i>protocol</i>	Protocol keywords; one of the following: <b>appletalk</b> , <b>bridge</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , <b>ipx</b> , <b>novell</b> , <b>snapshot</b> , <b>vines</b> , and <b>xns</b> .
<i>next-hop-address</i>	Protocol address used to match against addresses to which packets are destined. This argument is not used with the <b>bridge</b> protocol keyword.
<b>name</b> host-name	(Optional) Case-sensitive name or ID of the remote device (usually the host name). For routers with ISDN interfaces, if calling line identification—sometimes called <i>CLI</i> , but also known as <i>caller ID</i> and <i>automatic number identification</i> (ANI)—is provided, the <i>host-name</i> field can contain the number that the calling line ID provides.
<b>spc</b>	(Optional) Semipermanent connection between customer equipment and the exchange; used only in Germany to configure connections between an ISDN BRI and a 1TR6 ISDN switch type.
<b>speed 56</b>   <b>speed 64</b>	(Optional) Line speed in kilobits per second to use. Used for ISDN only. The default is <b>speed 64</b> (64 kbps).
<b>broadcast</b>	(Optional) Broadcasts should be forwarded to this protocol address.
<b>class</b> class-name	Name of the class that configures the ISDN AOC static dialer timeout period or the short-hold timeout period or both.
<i>dial-string[:isdn-subaddress]</i>	(Optional) Telephone number and optional ISDN subaddress used for ISDN multipoint connections that are sent to the dialing device when it recognizes packets with the specified next hop address that matches the access lists defined. The dial string and ISDN subaddress, if used, must be the last item in the command line.

## dialer map (SPC)

To set up network addressing on an ISDN BRI interface to support semipermanent connections (if the ISDN switch supports such connections), use the following form of the **dialer map** interface configuration command. To delete a particular dialer map entry, use the **no** form of this command.

```
dialer map protocol next-hop-address [name host-name] [spc] [speed 56 | speed 64] [broadcast]
dial-string[:isdn-subaddress]
```

```
no dialer map protocol next-hop-address [name host-name] [spc] [speed 56 | speed 64]
[broadcast] dial-string[:isdn-subaddress]
```

Syntax Description	
<i>protocol</i>	Protocol keywords; one of the following: <b>appletalk</b> , <b>bridge</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , <b>ipx</b> , <b>novell</b> , <b>snapshot</b> , <b>vines</b> , and <b>xns</b> .
<i>next-hop-address</i>	Protocol address used to match against addresses to which packets are destined. This argument is not used with the <b>bridge</b> protocol keyword.
<b>name</b> <i>host-name</i>	(Optional) Case-sensitive name or ID of the remote device (usually the host name). For routers with ISDN interfaces, if calling line identification—sometimes called <i>CLI</i> , but also known as <i>caller ID</i> and <i>automatic number identification</i> (ANI)—is provided, the <i>host-name</i> field can contain the number that the calling line ID provides.
<b>spc</b>	(Optional) Semipermanent connection between customer equipment and the exchange; used only in Germany to configure connections between an ISDN BRI and a 1TR6 ISDN switch type.
<b>speed 56</b>   <b>speed 64</b>	(Optional) Line speed in kilobits per second to use. Used for ISDN only. The default speed is 64 kbps.
<b>broadcast</b>	(Optional) Broadcasts are forwarded to this protocol address.
<i>dial-string[:isdn-subaddress]</i>	(Optional) Telephone number and optional ISDN subaddress used for ISDN multipoint connections that are sent to the dialing device when it recognizes packets with the specified next hop address that matches the access lists defined. The dial string and ISDN subaddress, if used, must be the last item in the command line.

## dialer map snapshot

To define a dialer map for Cisco's snapshot routing protocol on a client router connected to a dial-on-demand routing (DDR) interface, use the **dialer map snapshot** interface configuration command. To delete one or more previously defined snapshot routing dialer maps, use the **no** form of this command.

```
dialer map snapshot sequence-number dial-string
```

```
no dialer map snapshot [sequence-number]
```

<b>Syntax Description</b>	<i>sequence-number</i>	A number in the range from 1 to 254, inclusive, that uniquely identifies a dialer map. (Optional for the <b>no</b> form.)
	<i>dial-string</i>	Telephone number of a remote snapshot server to be called during an active period.

## dialer max-link

To specify the maximum number of links to a remote destination that can be up at any one time for a dialer profile, use the **dialer max-link** interface configuration command.

**dialer max-link** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of links, in the range 1 through 255. Default is 255 links.
---------------------------	---------------	--

## dialer outgoing

To configure the dialer map class for a Network Specific Facilities (NSF) dialing plan to support outgoing calls, use the **dialer outgoing** map-class dialer configuration command.

**dialer outgoing** *class-name*

<b>Syntax Description</b>	<i>class-name</i>	Keyword for a specified AT&T Primary-4ESS NSF dialing plan. The following keywords are supported: <b>sdn</b> , <b>megacomm</b> , and <b>accunet</b> .
---------------------------	-------------------	---

## dialer pool

To specify, for a dialer interface, which dialing pool to use to connect to a specific destination subnetwork, use the **dialer pool** interface configuration command. To remove the dialing pool assignment, use the **no** form of this command.

**dialer pool** *number*

**no dialer pool** *number*

<b>Syntax Description</b>	<i>number</i>	Dialing pool number, in the range 1 through 255.
---------------------------	---------------	--

## dialer pool-member

To configure a physical interface to be a member of a dialer profile dialing pool, use the **dialer pool-member** interface configuration command. To remove the configuration, use the **no** form of this command.

**dialer pool-member** *number* [**priority** *priority*] [**min-link** *minimum*] [**max-link** *maximum*]

**no dialer pool-member** *number*

### Syntax Description

<b>number</b>	Dialing pool number, in the range 1 through 255.
<b>priority</b> <i>priority</i>	(Optional) Priority of this interface within the dialing pool, in the range 0 (lowest) to 255 (highest). Interfaces with the highest priority are selected first for dialing out. Default is 0.
<b>min-link</b> <i>minimum</i>	(Optional) Minimum number of B channels on this interface that are reserved for this dialing pool, in the range 0 to 255. Default is 0. A reserved channel is inactive until the specified interface uses it to place calls. Applies to ISDN interfaces only.
<b>max-link</b> <i>maximum</i>	(Optional) Maximum number of B channels on this interface that can be used by this dialing pool, in the range 0 to 255. Default is 255. Applies to ISDN interfaces only.

## dialer priority

To set the priority of an interface in a dialer rotary group, use the **dialer priority** interface configuration command. To revert to the default setting, use the **no** form of this command.

**dialer priority** *number*

**no dialer priority**

### Syntax Description

<b>number</b>	Priority of an interface in a dialer rotary group; the highest number indicates the highest priority. This is a number from 0 through 255. The default value is 0, the lowest priority.
---------------	---

## dialer redial

To configure redial after failed outbound dial attempts, use the **dialer redial** command in interface configuration mode. To disable redial, use the **no** form of this command.

**dialer redial interval** *time* **attempts** *number* [**re-enable** *disable-time*]

**no dialer redial**

Syntax Description		
<b>interval</b> <i>time</i>		Time, in seconds, between redial attempts. The time can range from 5 to 2147483 seconds.
<b>attempts</b> <i>number</i>		The maximum number of redial attempts to be performed. The number can range from 1 to 2147483.
<b>re-enable</b> <i>disable-time</i>		(Optional) Time, in seconds, for which the interface will be disabled if all redial attempts fail. The time can range from 5 to 2147483 seconds.

## dialer remote-name

To specify the authentication name of the remote router on the destination subnetwork for a dialer interface, use the **dialer remote-name** interface configuration command. To remove the specified name, use the **no** form of this command.

**dialer remote-name** *user-name*

**no dialer remote-name**

Syntax Description		
<i>user-name</i>		Case-sensitive character string identifying the remote device; maximum length is 255 characters.

## dialer reserved-links

To reserve links for dial-in and dial-out, use the **dialer reserved-links** interface configuration command. To clear the link, use the **no** form of this command.

**dialer reserved-links** {*dialin-link* | *dialout-link*}

**no dialer reserved-links**

Syntax Description		
<i>dialin-link</i>		Link reserved for dial-in.
<i>dialout-link</i>		Link reserved for dial-out.

## dialer rotary-group

To include a specified interface in a dialer rotary group, use the **dialer rotary-group** interface configuration command. To remove the specified interface, use the **no** form of this command.

**dialer rotary-group** *number*

**no dialer rotary-group** *number*

<b>Syntax Description</b>	<i>number</i>	Number of the previously defined dialer interface in whose rotary group this interface is to be included. This is a number from 0 to 255. The dialer interface is defined by the <b>interface dialer</b> command.
---------------------------	---------------	---

## dialer rotor

To specify the method for identifying the outbound line to be used for ISDN or asynchronous dial-on-demand routing (DDR) calls, use the **dialer rotor** interface configuration command. To remove the specified method, use the **no** form of this command.

**dialer rotor** {**priority** | **best**}

**no dialer rotor** {**priority** | **best**}

<b>Syntax Description</b>	<b>priority</b>	Selects the first outbound line with the highest priority; this is the selection criterion that was previously used.
	<b>best</b>	Selects the outbound line with the most recent success. If that line also has the most recent failure, then it will try the line with the least recent failure. If that line also has the most recent failure, it will then try an as-of-yet untried outbound line.

## dialer string

To specify the string (telephone number) to be called for interfaces calling a single site, use the **dialer string** interface configuration command. To delete the dialer string specified for the interface, use the **no** form of this command.

**dialer string** *dial-string[:isdn-subaddress]*

**no dialer string**

<b>Syntax Description</b>	<i>dial-string</i>	String of characters to be sent to a DCE device.
	<i>:isdn-subaddress</i>	(Optional) ISDN subaddress.

## dialer string (dialer profiles)

To specify the string (telephone number) to be used when placing a call from an interface, use the **dialer string** interface configuration command. To delete the telephone number specified for the interface, use the **no** form of this command.

**dialer string** *dial-string* [**class** *class-name*]

**no dialer string**

**Syntax Description**

<i>dial-string</i>	Telephone number to be sent to a DCE device.
<b>class</b> <i>class-name</i>	(Optional) Dialer map class associated with this telephone number.

## dialer string (legacy DDR)

To specify the destination string (telephone number) to be called for interfaces calling a single site, use the **dialer string** interface configuration command. To delete the dialer string specified for the interface, use the **no** form of this command.

**dialer string** *dial-string[:isdn-subaddress]*

**no dialer string**

**Syntax Description**

<i>dial-string</i>	String of characters to be sent to a DCE device.
<i>:isdn-subaddress</i>	(Optional) ISDN subaddress.

## dialer voice-call

To configure the dialer map class for a Network Specific Facilities (NSF) dialing plan to support outgoing voice calls, use the **dialer voice-call** map-class dialer configuration command.

**dialer voice-call**

**Syntax Description**

This command has no arguments or keywords.

## dialer vpdn

To enable a dialer profile or dial-on-demand routing (DDR) dialer to use Layer 2 Tunnel Protocol (L2TP) dialout, use the **dialer vpdn** interface configuration command. To disable L2TP dialout on a dialer profile or DDR dialer, use the **no** form of this command.

**dialer vpdn**

**no dialer vpdn**

**Syntax Description**

This command has no arguments or keywords.

## dialer wait-for-carrier-time (interface configuration)

To specify the length of time the interface waits for a carrier, use the **dialer wait-for-carrier-time** interface configuration command. To reset the carrier wait time value to the default, use the **no** form of this command.

**dialer wait-for-carrier-time** *seconds*

**no dialer wait-for-carrier-time**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds that the interface waits for the carrier to come up when a call is placed. Acceptable values are positive, nonzero integers.
---------------------------	----------------	--

## dialer wait-for-carrier-time (map-class dialer configuration)

To specify the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class, use the **dialer wait-for-carrier-time** map-class dialer configuration command. To reset the carrier wait time value to the default, use the **no** form of this command.

**dialer wait-for-carrier-time** *seconds*

**no dialer wait-for-carrier-time**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds that the interface waits for the carrier to come up when a call is placed. Acceptable values are positive, nonzero integers. The default is 30 seconds.
---------------------------	----------------	---

## dialer watch-disable

To set a delay time to the backup interface, use the **dialer watch-disable** interface configuration command. To disable this feature, use the **no** form of this command.

**dialer watch-disable** *timeout*

**no dialer watch-disable**

<b>Syntax Description</b>	<i>timeout</i>	The timeout value in seconds.
---------------------------	----------------	-------------------------------

## dialer watch-group

To enable dial-on-demand routing (DDR) backup on an interface using Dialer Watch, configure the interface using the **dialer watch-group** interface configuration command. To disable this feature, use the **no** form of this command.

```
dialer watch-group group-number
```

```
no dialer watch-group group-number
```

### Syntax Description

<i>group-number</i>	Group number assigned that will point to a globally defined list of IP addresses to watch. The valid range is 1 to 255.
---------------------	---

## dialer watch-list

To add to the list of IP addresses to be monitored for Dialer Watch or to configure the router to dial the backup link if the primary link fails during initial startup, use the **dialer watch-list** global configuration command. To disable these features, use the **no** form of this command.

```
dialer watch-list group-number {ip ip-address address-mask | delay route-check initial time}
```

```
no dialer watch-list group-number {ip ip-address address-mask | delay route-check initial time}
```

### Syntax Description

<i>group-number</i>	Group number assigned to the list. Valid group numbers are between 1 and 255.
<b>ip</b>	IP is the only routed protocol supported for Dialer Watch.
<i>ip-address</i>	IP address or address range to be applied to the list.
<i>address-mask</i>	IP address mask to be applied to the list.
<b>delay route-check initial time</b>	Time, in seconds, after which the router ensures that the primary route is up once initial startup is complete.

## dial-peer cor custom

To specify that named class of restrictions (COR) apply to dial peers, use the **dial-peer cor custom** global configuration command.

```
dial-peer cor custom
```

### Syntax Description

This command has no arguments or keywords.

## dial-peer cor list

To define a class of restrictions (COR) list name, use the **dial-peer cor list** global configuration command. To remove a previously defined COR list name, use the **no** form of this command.

**dial-peer cor list** *list-name*

**no dial-peer cor list** *list-name*

Syntax Description	<i>list-name</i>
	List name that is applied to incoming or outgoing calls to specific numbers or exchanges.

## dial-shelf split backplane-ds0

To connect two router shelves to a dial shelf, use the **dial-shelf split backplane-ds0** global configuration command. To remove the connection, use the **no** form of this command.

**dial-shelf split backplane-ds0** {*predefined-option* | **userdefined** *option*}

**no dial-shelf split backplane-ds0**

Syntax Description	<i>predefined-option</i>
	Predefined backplane DS-0 pairs. See Table 39 for a list of these options.
	<b>userdefined</b> <i>option</i>
	Number of backplane DS-0 interfaces used by the router shelf that you define, in the range 128 to 2048.

**Table 39** *dial-shelf split backplane ds-0 Predefined Options*

Option Pair	Router Shelf 1			Router Shelf 2			Total
	Option	Maximum Calls	Unused T1	Option	Maximum Calls	Unused T1	
1	2ct3cas	1344		1ct3cas	672		2016
2	part2ct1ct3cas	1152	4	part1ct1ct3cas	888	3	2040
3	2ct3isdn	1288		part1ct1ct3isdn_b	644	7	1932
4	part2ct1ct3isdn	1150	2	part1ct1ct3isdn	897	1	2047
5 <sup>1</sup>	3ce1	960		3ce1	960		1920
6	Default (no option entered)	1/2 of current input		Default (no option entered)	1/2 of current input		
7	<b>no dial-shelf backplane-ds0</b>	1024		<b>no dial-shelf backplane-ds0</b>	1024		2048

1. This option is used to revert to the default for an environment that uses six E1 lines.

## dial-shelf split slots

To configure split dial shelves, use the **dial-shelf split slots** global configuration command. To change the router shelf to normal mode, if a router is in split mode and the other router shelf has already relinquished control of all dial shelf slots or is switched off, use the **no** form of this command.

**dial-shelf split slots** *slot-numbers*

**no dial-shelf split slots**

---

**Syntax Description**

*slot-numbers* List of the dial shelf slot numbers that the router owns in the range 0 to 11, separated by spaces. Slot ownership for each of the two router shelves is configured individually using the **dial-shelf split slots** command.

---

## dial-shelf split slots none

To configure the router in dial shelf split mode but with no slots owned, use the **dial-shelf split slots none** global configuration command.

**dial-shelf split slots none**

---

**Syntax Description**

This command has no arguments or keywords.

## dial-shelf split slots remove

To remove slots configured in split mode, use the **dial-shelf split slots remove** global configuration command.

**dial-shelf split slots remove** *slot-numbers*

---

**Syntax Description**

*slot-numbers* List of the dial shelf slot numbers to be removed, separated by spaces, in the range 0 to 11.

---

## dial-tdm-clock

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the dial shelf of the Cisco AS5800, use the **dial-tdm-clock** global configuration command. To return the clock source and priority to the default values, use the **no** form of this command.

**dial-tdm-clock priority** *number* { **external** { **e1** | **t1** } [**120ohm**] | **freerun** | **trunk-slot** *slot* **port** *port* }

**no dial-tdm-clock priority** *number* { **external** { **e1** | **t1** } [**120ohm**] | **freerun** | **trunk-slot** *slot* **port** *port* }

Syntax Description		
<b>priority</b> <i>number</i>	Priority of the clock source. The range is 1 to 50. Priority 1 is the highest priority and 50 is the lowest.	
<b>external</b>	Priority of an external clock source. The external clock source is connected to the front panel of the dial shelf controller (DSC) card.	
{ <b>e1</b>   <b>t1</b> } [ <b>120ohm</b> ]	Priority of the E1 (2.048 MHz) or T1 (1.54 MHz) external clock source. The default value of the external coaxial cable impedance is 75 ohms. Specify the <b>120ohm</b> option if a 120 ohms coaxial cable is connected.	
<b>freerun</b>	Priority of the local oscillator clock source.	
<b>trunk-slot</b> <i>slot</i>	Priority of the trunk card to provide the clock source. The slot number is from 0 to 5 (these are the only slots capable of providing clock sources).	
<b>port</b> <i>port</i>	Controller number on the trunk used to provide the clock source. The port number is from 0 to 28. The T1 and E1 trunk cards each have 12 ports. The T3 trunk card has 28 ports.	

## disconnect

To disconnect a line, use the **disconnect** EXEC command.

**disconnect** [*connection*]

Syntax Description		
<i>connection</i>	(Optional) Number of the line or name of the active network connection to be disconnected.	

## dnis

To support additional Dialed Number Identification Service (DNIS) groups for a specific VPDN tunnel, use the **dnis** VPDN group configuration command. To remove a DNIS from a VPDN group, enter the **no** form of this command.

**dnis** *dnis-group-name*

**no dnis** *dnis-group-name*

**dnis** *dnis-number*

**no dnis** *dnis-number*

**Note**

When Resource Pool Management (RPM) is enabled, this command uses the *dnis-group-name* argument. When RPM is disabled, this command uses the *dnis-number* argument.

**Syntax Description**

<i>dnis-group-name</i>	DNIS group name used when RPM is enabled and the VPDN group is configured under the incoming customer profile.
<i>dnis-number</i>	DNIS group number used when RPM is disabled, or when a call is associated with a customer profile without any VPDN group configured for the customer profile.

## dnis group

To include a group of Dialed Number Identification Service (DNIS) numbers in a customer profile, use the **dnis group** customer profile configuration command. To remove a DNIS group from a customer profile, use the **no** form of this command.

**dnis group** { **default** | **name** *name* }

**no dnis group** { **default** | **name** *name* }

**Syntax Description**

<b>default</b>	Allows a specified customer profile to accept all DNIS numbers coming into the access server. For example, a stray DNIS number not listed in any customer profile passes through this default DNIS group. Most customer profiles do not have this option configured.
<b>name</b>	Assigns a name to a DNIS group.
<i>name</i>	DNIS group name. It can have up to 23 characters.

## domain

To request that PPP calls from a specific domain name be tunneled, or to support additional domain names for a specific virtual private dialup network (VPDN) group, use the **domain** request-dialin or VPDN group configuration command. To remove a domain from a VPDN group or subgroup, use the **no** form of this command.

**domain** *domain-name*

**no domain** [*domain-name*]

**Syntax Description**

<i>domain-name</i>	Case-sensitive name of the domain that will be tunneled.
--------------------	--

## ds0 busyout

To busyout one or more digital signal level 0s (DS0s), use the **ds0 busyout** controller configuration command. To cancel busyout on a DS0, use the **no** form of this command.

**ds0 busyout** *ds0*

**no ds0 busyout** *ds0*

<b>Syntax Description</b>	<i>ds0</i>	DS0 number listed as a single channel or channel range. The range of numbers can be from 1 to 24 for T1. For example, from 1 to 10, or from 10 to 24.
---------------------------	------------	---

## ds0 busyout-threshold

To define a threshold to maintain a balance between the number of DS0s and modems, use the **ds0 busyout-threshold** global configuration command. To remove the threshold, use the **no** form of this command.

### Cisco AS5300 and AS5800 Access Servers Only

**ds0 busyout-threshold** *threshold-number*

**no ds0 busyout-threshold** *threshold-number*



#### Note

This command is the same as the **modem busyout-threshold** command for the Cisco AS5350 and AS5400 access servers.

<b>Syntax Description</b>	<i>threshold-number</i>	Number of modems that are free when the router should enforce the stipulation that the number of free DS0 lines is less than or equal to the number of modems.
---------------------------	-------------------------	--

## ds0-group (controller e1)

To define E1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN, enter the **ds0-group** controller configuration command. To remove the group and signaling setting, use the **no** form of this command.

**ds0-group** *channel timeslots range type signal*

**no ds0-group** *channel timeslots range type signal*

**Syntax Description**

<i>channel</i>	Specifies a single channel group number. Replace the <i>channel</i> variable with a number from 0 through 30.
<b>timeslots</b> <i>range</i>	Specifies a time-slot range, which can be from 1 through 31. You can specify a time-slot range (for example, 1-31), individual time-slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). The sixteenth time slot is reserved for out-of-band signaling.
<b>type</b> <i>signal</i>	Specifies the type of channel-associated signaling. Configure the signal type that your central office uses. Replace the <i>signal</i> argument with one of the following signal types: <ul style="list-style-type: none"> <li>• <b>r2-analog</b> [<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]]</li> <li>• <b>r2-digital</b> [<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]]</li> <li>• <b>r2-pulse</b> [<b>r2-compelled</b> [ani]   <b>r2-non-compelled</b> [ani]   <b>r2-semi-compelled</b> [ani]]</li> </ul>

The following descriptions are provided for the previous three R2 syntax bullets:

**r2-analog**—Specifies R2 ITU Q411 analog line signaling, which reflects the on/off switching of a tone in frequency-division multiplexing circuits (before TDM circuits were created). The tone is used for line signaling.

**r2-digital**—Specifies R2 ITU Q421 digital line signaling, which is the most common signaling configuration. The A and B bits are used for line signaling.

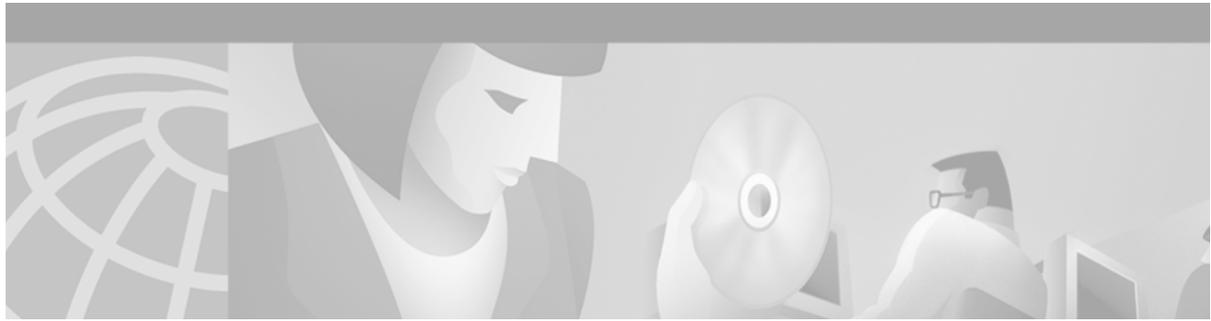
**r2-pulse**—Specifies R2 ITU supplement 7 pulse line signaling, which is a transmitted pulse that indicates a change in the line state.

**r2-compelled** [ani]—Specifies R2 compelled register signaling. You can also specify provisioning the ANI address option.

**r2-non-compelled** [ani]—Specifies R2 noncompelled register signaling.

**r2-semi-compelled** [ani]—Specifies R2 semicompelled register signaling.

■ ds0-group (controller e1)



## Dial Technologies Commands: encapsulation cpp Through modem-pool

---

This chapter describes the function and syntax of the dial technologies commands: **encapsulation cpp** through **modem-pool**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Dial Technologies Command Reference*.

### encapsulation cpp

To enable encapsulation for communication with routers or bridges using the Combinet Proprietary Protocol (CPP), use the **encapsulation cpp** interface configuration command. To disable CPP encapsulation, use the **no** form of this command.

**encapsulation cpp**

**no encapsulation cpp**

---

**Syntax Description** This command has no arguments or keywords.

### encryption mppe

To enable Microsoft Point-to-Point Encryption (MPPE) on an Industry-Standard Architecture (ISA) card, use the **encryption mppe** ISA controller configuration command. To disable MPPE, use the **no** form of this command.

**encryption mppe**

**no encryption mppe**

---

**Syntax Description** This command has no arguments or keywords.

## firmware location

To download firmware into the modems, use the **firmware location** command in Service Processing Element (SPE) configuration mode. Use the **no** form of this command to revert the router back to the system embedded image default.

**firmware location** {**system** | **flash**}: *filename*

**no firmware location** {**system** | **flash**}: *filename*

### Syntax Description

<b>system</b>	Router loads the firmware from a built-in file within the Cisco IOS image.
<b>flash</b>	Router loads the firmware from the Flash NVRAM located within the router.
<i>filename</i>	The name of the desired firmware file. If system is specified, enter the path to the filename you want to download.

## firmware upgrade

To modify the way in which the Service Processing Element (SPE) will be downloaded, use the **firmware upgrade** SPE configuration command. To revert to the default SPE firmware upgrade option, busyout, use the **no** form of this command.

**firmware upgrade** {**busyout** | **recovery** | **reboot**}

**no firmware upgrade**

### Syntax Description

<b>busyout</b>	Upgrades when all calls are terminated on the SPE.
<b>recovery</b>	Upgrades during download maintenance time.
<b>reboot</b>	Upgrades at the next reboot.

## flowcontrol

To set the method of data flow control between the terminal or other serial device and the router, use the **flowcontrol** line configuration command. To disable flow control, use the **no** form of this command.

**flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

**no flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

### Syntax Description

<b>none</b>	Turns off flow control.
<b>software</b>	Sets software flow control. An optional keyword specifies the direction: <b>in</b> causes the Cisco IOS software to listen to flow control from the attached device, and <b>out</b> causes the software to send flow control information to the attached device. If you do not specify a direction, both are assumed.

<b>lock</b>	(Optional) Makes it impossible to turn off flow control from the remote host when the connected device <i>needs</i> software flow control. This option applies to connections using the Telnet or rlogin protocols.
<b>hardware</b> <b>[in   out]</b>	Sets hardware flow control. An optional keyword specifies the direction: <b>in</b> causes the software to listen to flow control from the attached device, and <b>out</b> causes the software to send flow control information to the attached device. If you do not specify a direction, both are assumed. For more information about hardware flow control, see the hardware manual that was shipped with your router.

## force-local-chap

To force the L2TP network server (LNS) to reauthenticate the client, use the **force-local-chap** VPDN group configuration command. To disable reauthentication, use the **no** form of this command.

**force-local-chap**

**no force-local-chap**

**Syntax Description** This command has no arguments or keywords.

## framing

To select the frame type for the T1 or E1 data line, use the **framing** controller configuration command. To turn off framing, use the **no** form of this command.

### T1 Line

**framing** {**sf** | **esf**}

**no framing**

### E1 Line

**framing** {**crc4** | **no-crc4**} [**australia**]

**no framing**

### Syntax Description

<b>sf</b>	Super Frame as the T1 frame type.
<b>esf</b>	Extended Super Frame as the T1 frame type.
<b>crc4</b>	CRC4 frame as the E1 frame type.
<b>no-crc4</b>	No CRC4 frame as the E1 frame type.
<b>australia</b>	(Optional) E1 frame type used in Australia.

## group-range

To create a list of member asynchronous interfaces (associated with a group interface), use the **group-range** interface configuration command. To remove an interface from the member list, use the **no** form of this command.

**group-range** *low-end-of-interfacerange high-end-of-interfacerange*

**no group-range** *interface*

Syntax Description		
	<i>low-end-of-interfacerange</i>	Beginning interface number to be made a member of the group interface.
	<i>high-end-of-interfacerange</i>	Ending interface number to be made a member of the group interface.
	<i>interface</i>	Interface number to be removed from the group interface.

## hw-module slot

To enable the router shelf to stop a Dial Shelf Controller (DSC) card, to restart a stopped DSC card, or to cause a reload of any specified dial shelf feature board, use the **hw-module slot** privileged EXEC command.

**hw-module slot** *shelf-id/slot-number* {**start** | **stop** | **reload**}

Syntax Description		
	<i>shelf-id</i>	Dial shelf number. The default shelf ID for the dial shelf is 1. You must type in the forward slash (/) as part of the command.
	<i>slot-number</i>	Number of the slot in the shelf where the target feature board or DSC is installed. If the <b>start</b> or <b>stop</b> keywords are used, the slot number must be either 12 or 13, as these keywords apply only to DSCs.
	<b>start</b>	Restarts the specified DSC.
	<b>stop</b>	Stops the specified DSC.
	<b>reload</b>	Enables a remote reload of an individual feature board without having to use manual online insertion and removal (OIR).

## initiate-to

To specify the IP address that will be tunneled to, use the **initiate-to** VPDN group configuration command. To remove an IP address from the VPDN group, use the **no** form of this command.

**initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]

**no initiate-to** [**ip** *ip-address*]

Syntax Description		
<b>ip</b> <i>ip-address</i>		IP address of the router that will be tunneled to.
<b>limit</b> <i>limit-number</i>		(Optional) Maximum number of connections that can be made to this IP address.
<b>priority</b> <i>priority-number</i>		(Optional) Priority for this IP address (1 is the highest).

## interface (RLM server)

To define the IP addresses of the Redundant Link Manager (RLM) server, use the **interface** interface configuration command. To disable this function, use the **no** form of this command.

**interface** *name-tag*

**no interface** *name-tag*

Syntax Description		
<i>name-tag</i>		Name to identify the server configuration so that multiple entries of server configuration can be entered.

## interface bri

To configure a BRI interface and enter interface configuration mode, use the **interface bri** global configuration command.

### Cisco 7200 Series and 7500 Series Routers Only

**interface bri** *number*

**interface bri** *slot/port*

### Cisco 7200 Series and 7500 Series Routers with BRI Subinterfaces Only

**interface bri** *number.subinterface-number* [**multipoint** | **point-to-point**]

**interface bri** *slot/port.subinterface-number* [**multipoint** | **point-to-point**]

### X.25 on an ISDN BRI Interface

**interface bri** *number:0*

**interface bri** *slot/port:0*

Syntax Description		
<i>number</i>		Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the <b>show interfaces</b> command.
<i>slot/port</i>		On the Cisco 7200 series, slot location and port number of the interface.

<i>.subinterface-number</i>	Subinterface number in the range 1 to 4,294,967,293. The <i>number</i> that precedes the period (.) must match the <i>number</i> this subinterface belongs to.
<b>multipoint</b>   <b>point-to-point</b>	(Optional) Specifies a multipoint or point-to-point subinterface. The default is <b>multipoint</b> .
<b>:0</b>	Subinterface created by applying the <b>isdn x25 static-tei</b> and the <b>isdn x25 dchannel</b> commands to the specified BRI interface. This interface must be configured for X.25.

## interface dialer

To define a dialer rotary group, use the **interface dialer** global configuration command.

```
interface dialer number
```

<b>Syntax Description</b>	<i>number</i>	Number of the dialer rotary group in the range 0 through 255.
---------------------------	---------------	---

## interface multilink

To create a multilink bundle or enter multilink interface configuration mode, use the **interface multilink** global configuration command. To remove a multilink bundle, use the **no** form of this command.

```
interface multilink group-number
```

```
no interface multilink
```

<b>Syntax Description</b>	<i>group-number</i>	Number of the multilink bundle (a nonzero number).
---------------------------	---------------------	--

## interface serial

To specify a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, channel-associated signalling, or robbed-bit signalling), use the **interface serial** global configuration command.

### Cisco 7200 Series and Cisco 7500 Series Routers

```
interface serial slot/port:timeslot
```

### Cisco AS5200 Series and Cisco 4000 Series Access Servers

```
interface serial number:timeslot
```

<b>Syntax Description</b>	<i>slot/port</i>	Slot number and port number where the channelized E1 or T1 controller is located.
	<i>:timeslot</i>	For ISDN, the D channel time slot, which is <b>:23</b> channel for channelized T1 and the <b>:15</b> for channelized E1. PRI time slots are in the range 0 to 23 for channelized T1 and in the range 0 to 30 for channelized E1.  For channel-associated signalling or robbed-bit signalling, the channel group number.  The colon (:) is required.  On a dual port card, it is possible to run channelized on one port and primary rate on the other port.
	<i>number</i>	Channelized E1 or T1 controller number.

## interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** global configuration command.

```
interface virtual-template number
```

<b>Syntax Description</b>	<i>number</i>	Number used to identify the virtual template interface.
---------------------------	---------------	---

## ip address negotiated

To specify that the IP address for a particular interface is obtained via PPP/IPCPC (IP Control Protocol) address negotiation, use the **ip address negotiated** interface configuration command. To disable this feature, use the **no** form of this command.

```
ip address negotiated
```

```
no ip address negotiated
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## ip address-pool

To enable an address pooling mechanism used to supply IP addresses to dialin asynchronous, synchronous, or ISDN point-to-point interfaces, use the **ip address-pool** global configuration command. To disable IP address pooling globally on all interfaces with the default configuration, use the **no** form of this command.

```
ip address-pool [dhcp-proxy-client | local]
```

```
no ip address-pool
```

Syntax Description		
<b>dhcp-proxy-client</b>	(Optional)	Uses the router as the proxy-client between a third-party Dynamic Host Configuration Protocol (DHCP) server and peers connecting to the router.
<b>local</b>	(Optional)	Uses the local address pool named <i>default</i> .

## ip dhcp-server

To specify which Dynamic Host Configuration Protocol (DHCP) servers to use on your network, or to specify the IP address of one or more DHCP servers available on the network, use the **ip dhcp-server** global configuration command. To remove a DHCP server IP address, use the **no** form of this command.

**ip dhcp-server** [*ip-address* | *name*]

**no ip dhcp-server** [*ip-address* | *name*]

Syntax Description		
<i>ip-address</i>	(Optional)	IP address of a DHCP server.
<i>name</i>	(Optional)	Name of a DHCP server.

## ip route

To establish static routes and define the next hop for large-scale dial-out, use the **ip route** global configuration command. To remove static routes, use the **no** form of this command.

**ip route** *network-number network-mask* {*ip-address* | *interface*} [*distance*] [**name** *name*]

**no ip route**

Syntax Description		
<i>network-number</i>		IP address of the target network or subnet.
<i>network-mask</i>		Network mask that lets you mask network and subnetwork bits.
<i>ip-address</i>		Internet address of the next hop that can be used to reach that network in standard IP address notation. Example: 10.1.1.1.
<i>interface</i>		Network interface to use.
<i>distance</i>	(Optional)	Administrative distance, which is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers.
<b>name</b> <i>name</i>	(Optional)	Name of the user profile.

## ip rtp reserve

To reserve a special queue for a set of Real-time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **ip rtp reserve** interface configuration command. To disable the special queue for real-time traffic, use the **no** form of this command.

**ip rtp reserve** *lowest-udp-port range-of-ports* [*maximum-bandwidth*]

**no ip rtp reserve**

Syntax Description		
<i>lowest-udp-port</i>		Lowest UDP port number to which the packets are sent.
<i>range-of-ports</i>		Number, which added to the lowest-UDP-port value, yields the highest UDP port value.
<i>maximum-bandwidth</i>		(Optional) Bandwidth, in kilobits per second, reserved for the RTP packets to be sent to the specified UDP ports.

## ip tcp async-mobility server

To enable asynchronous listening, which in turn allows TCP connections to TCP port 57, use the **ip tcp async-mobility server** global configuration command. To turn listening off, use the **no** form of this command.

**ip tcp async-mobility server**

**no ip tcp async-mobility server**

**Syntax Description** This command has no arguments or keywords.

## ip telnet quiet

To suppress the display of Telnet connection messages, use the **ip telnet quiet** global configuration command. To cancel this option, use the **no** form of this command.

**ip telnet quiet**

**no ip telnet quiet**

**Syntax Description** This command has no arguments or keywords.

## ipx compression cipx

To enable compression of Internetwork Packet Exchange (IPX) packet headers in a PPP session, use the **ipx compression cipx** interface configuration command. To disable compression of IPX packet headers in a PPP session, use the **no** form of this command.

**ipx compression cipx** *number-of-slots*

**no ipx compression cipx**

<b>Syntax Description</b>	<i>number-of-slots</i>	Number of stored IPX headers allowed. The range is from 10 to 256. The default is 16.
<p>A slot is similar to a table entry for a complete IPX header. When a packet is received, the receiver stores the complete IPX header in a slot and tells the destination which slot it used. As subsequent CIPX packets are sent, the receiver uses the slot number field to determine which complete IPX header to associate with the CIPX packet before passing the packet up to IPX.</p>		

## ipx ppp-client

To enable a nonrouting Internetwork Packet Exchange (IPX) client to connect to an asynchronous interface, the interface must be associated with a loopback interface configured to run IPX. To permit such connections, use the **ipx ppp-client** interface configuration command. To disable a nonrouting IPX client, use the **no** form of this command.

**ipx ppp-client loopback** *number*

**no ipx ppp-client loopback** *number*

<b>Syntax Description</b>	<b>loopback</b>	Loopback interface configured with a unique IPX network number.
<i>number</i>		Number of the loopback interface.

## isdn all-incoming-calls-v120

To configure an ISDN BRI or PRI interface to answer all incoming calls as V.120 when the terminal adapter uses V.120 signalling but does not send the Lower-Layer Compatibility field in Setup messages, use the **isdn all-incoming-calls-v120** interface configuration command.

**isdn all-incoming-calls-v120**

**no isdn all-incoming-calls-v120**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## isdn answer1, isdn answer2

To have the router verify a called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer1** interface configuration command. To remove the verification request, use the **no** form of this command.

```
isdn answer1 [called-party-number][:subaddress]
```

```
no isdn answer1 [called-party-number][:subaddress]
```

To have the router verify an *additional* called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer2** interface configuration command. To remove this second verification request, use the **no** form of this command.

```
isdn answer2 [called-party-number][:subaddress]
```

```
no isdn answer2 [called-party-number][:subaddress]
```

Syntax Description		
	<i>called-party-number</i>	(Optional) Telephone number of the called party. At least one value— <i>called-party-number</i> or <i>subaddress</i> —must be specified. The maximum number of digits for <i>called-party-number</i> is 50.
	:	(Optional) Identifies the number that follows as a subaddress. Use the colon (: ) when you configure both the called party number and the subaddress, or when you configure only the subaddress.
	<i>subaddress</i>	(Optional) Subaddress number used for ISDN multipoint connections. At least one value— <i>called-party-number</i> or <i>subaddress</i> —must be specified. The maximum number of digits for <i>subaddress</i> is 50.

## isdn autodetect

To enable the automatic detection of ISDN SPIDs and switch type, use the **isdn autodetect** interface configuration command. To disable the automatic detection of ISDN SPIDs and switch type, use the **no** form of this command.

```
isdn autodetect
```

```
no isdn autodetect
```

Syntax Description	
	This command has no arguments or keywords.

## isdn bchan-number-order

To configure an ISDN PRI interface to make outgoing call selection in ascending or descending order, use the **isdn bchan-number-order** interface configuration command. To restore the default (descending order), use the **no** form of this command or simply reconfigure the interface with the new value.

```
isdn bchan-number-order {ascending | descending}
```

```
no isdn bchan-number-order
```

### Syntax Description

<b>ascending</b>	Makes the outgoing B channel selection in ascending order as follows: <ul style="list-style-type: none"> <li>• Channels 1 to 24 for a T1 controller</li> <li>• Channels 1 to 31 for an E1 controller</li> </ul>
<b>descending</b>	Makes the outgoing B channel selection in descending order as follows: <ul style="list-style-type: none"> <li>• Channels 24 to 1 for a T1 controller</li> <li>• Channels 31 to 1 for an E1 controller</li> </ul>

## isdn busy

To set a false busy signal on an ISDN B channel, use the **isdn busy** interface configuration command. To remove this condition, use the **no** form of this command.

```
isdn busy dsl number b_channel number
```

```
no isdn busy dsl number b_channel number
```

### Syntax Description

<b>dsl</b> <i>number</i>	Digital subscriber loop (DSL) number.
<b>b_channel</b> <i>number</i>	B channel or range of B channels to be set to the false busy signal. B channel numbers range from 1 to 24; 0 indicates the entire interface. The state of the channel, which is obtained using the <b>show isdn</b> command with the <b>status</b> keyword, can also be added to the command.

## isdn call interface

To make an ISDN data call, use the **isdn call interface** privileged EXEC command.

```
isdn call interface interface-number dialing-string [speed 56 | 64]
```

### Syntax Description

<i>interface-number</i>	Interface number.
<i>dialing-string</i>	Telephone number used for making ISDN data call.
<b>speed</b> <b>56</b>	(Optional) Line speed (56 or 64 kbps) used for making ISDN data call.
<b>speed</b> <b>64</b>	

## isdn caller

To configure ISDN caller ID screening and optionally to enable ISDN caller ID callback for legacy dial-on-demand routing (DDR), use the **isdn caller** interface configuration command. To disable this feature, use the **no** form of this command.

**isdn caller** *phone-number* [**callback**]

**no isdn caller** *phone-number* [**callback**]

<b>Syntax Description</b>	<i>phone-number</i>	Remote telephone number for which to screen. Use a letter X to represent a single “don’t care” digit. The maximum length of each number is 25 digits.
	<b>callback</b>	(Optional) Enable callback.

## isdn calling-number

To configure an ISDN PRI or BRI interface to present the number of the device making the outgoing call, use the **isdn calling-number** interface configuration command. To remove a previously configured calling number, use the **no** form of this command.

**isdn calling-number** *calling-number*

**no isdn calling-number**

<b>Syntax Description</b>	<i>calling-number</i>	Number of the device making the outgoing call; only one entry is allowed.
---------------------------	-----------------------	---

## isdn calling-pty

To specify whether the network-provided or user-provided calling party number is selected when two calling party numbers are sent from a primary NET5 switch on ISDN, use the **isdn calling-pty** interface configuration command. To reset the default value, use the **no** form of this command.

**isdn calling-pty** {**network-provided** | **user-provided**}

**no isdn calling-pty**

<b>Syntax Description</b>	<b>network-provided</b>	Network-provided calling party number.
	<b>user-provided</b>	User-provided calling party number.

## isdn conference-code

To activate three-way call conferencing, use the **isdn conference-code** interface configuration command. To disable three-way call conferencing, use the **no** form of this command.

**isdn conference-code** *range*

**no isdn conference-code**

Syntax Description	<i>range</i>
	Number from 0 to 999 (ISDN conference code).

## isdn disconnect-cause

To send a specific ISDN cause code to the switch, use the **isdn disconnect-cause** interface configuration command. To return to the default condition, use the **no** form of this command.

**isdn disconnect-cause** { *cause-code-number* | **busy** | **not-available** }

**no isdn disconnect-cause**

Syntax Description	<i>cause-code-number</i>	Sends a cause code number (submitted as integer in the range of 1 through 127) to the switch.
	<b>busy</b>	Sends the USER-BUSY code to the switch.
	<b>not-available</b>	Sends the CHANNEL-NOT-AVAILABLE code to the switch.

## isdn disconnect interface

To disconnect an ISDN data call without bringing down the interface, use the **isdn disconnect interface** privileged EXEC command.

**isdn disconnect interface** *interface-type interface-number* { **b1** | **b2** | **all** }

Syntax Description	<i>interface-type</i> <i>interface-number</i>	Interface type and number, such as bri 0.
	<b>b1</b>	B channel 1.
	<b>b2</b>	B channel 2.
	<b>all</b>	B channels 1 and 2.

## isdn fast-rollover-delay

To specify the time within which an incoming call is dropped before attempting to place the call back call, use the **isdn fast-rollover-delay** interface configuration command. To remove or change a value, use the **no** form of this command.

**isdn fast-rollover-delay** *seconds*

**no isdn fast-rollover-delay**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds to allow an incoming call to completely drop before placing the callback call.
---------------------------	----------------	--

## isdn gateway-max-interworking

To prevent the H.323 gateway from checking for ISDN protocol compatibility and dropping information elements (IEs) in call messages, use the **isdn gateway-max-interworking** global configuration command. To restore the default condition, use the **no** form of this command.

**isdn gateway-max-interworking**

**no isdn gateway-max-interworking**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--

## isdn guard-timer

To enable a managed timer for authentication requests, use the **isdn guard-timer** interface configuration command. To reset the timer to its default value, use the **no** form of this command.

**isdn guard-timer** *msecs* [**on-expiry** {**accept** | **reject**}]

**no isdn guard-timer**

<b>Syntax Description</b>	<i>msecs</i>	Number of milliseconds that the network access server (NAS) waits for a response from the AAA security server. The valid range is from 1000 through 20,000.
	<b>on-expiry</b>	(Optional) Determines whether calls are accepted or rejected after the specified number of milliseconds has expired. If no expiry action is selected, calls are rejected.
	<b>accept</b>	(Optional) Calls are accepted if the guard-timer expires before AAA responds.
	<b>reject</b>	(Optional) Calls are rejected if the guard-timer expires before AAA responds.

## isdn incoming-voice

To route all incoming voice calls to the modem and determine how they will be treated, use the **isdn incoming-voice** interface configuration command. To disable the setting or return to the default, use the **no** form of this command.

```
isdn incoming-voice { voice | data [56 | 64] | modem [56 | 64] }
```

```
no isdn incoming-voice { voice | data [56 | 64] | modem [56 | 64] }
```

### Syntax Description

<b>voice</b>	Incoming voice calls bypass the modems and be handled as a voice call.
<b>data</b>	Incoming voice calls bypass the modems and be handled as digital data. If this keyword is selected, you can specify a B-channel bandwidth of either <b>56</b> kbps or <b>64</b> kbps. If no argument is entered, the default value is 64.
<b>modem</b>	Incoming voice calls are passed over to the digital modems, where they negotiate the appropriate modem connection with the far-end modem. If this keyword is selected, you can specify a B-channel bandwidth of either <b>56</b> kbps or <b>64</b> kbps. If no argument is entered, the default value is 64.

## isdn layer1-emulate

To configure the Layer 1 operation of a BRI voice port as clock master (NT) or slave (TE), use the **isdn layer1-emulate** interface configuration command. To restore the default (user), use the **no** form of this command.

```
isdn layer1-emulate { user | network }
```

```
no isdn layer1-emulate
```

### Syntax Description

<b>user</b>	Physical interface operation in clock slave mode (as TE).
<b>network</b>	Physical interface operation in clock master mode (as NT).

## isdn leased-line bri 128

To configure an ISDN BRI for leased-line service at 128 kbps, use the **isdn leased-line bri 128** global configuration command. To remove the configuration, use the **no** form of this command.

```
isdn leased-line bri number 128
```

```
no isdn leased-line bri number 128
```

### Syntax Description

<i>number</i>	BRI interface number.
---------------	-----------------------

## isdn map

To override the default ISDN type and plan generated by the router with custom values, use the **isdn map** interface configuration command. To revert to the default ISDN type and plan, use the **no** form of this command.

```
isdn map {address address | regexp | plan plan | type type}
```

```
no isdn map {address address | regexp | plan plan | type type}
```

### Syntax Description

<b>address</b> <i>address</i>	Address map, which can be to either the calling or called number.
<i>regexp</i>	Regular expression for pattern matching.
<b>plan</b> <i>plan</i>	ISDN numbering plan.
<b>type</b> <i>type</i>	ISDN number type.

## isdn negotiate-bchan

To enable the router to accept a B channel that is different from the B channel requested in the outgoing call setup message, use the **isdn negotiate-bchan** interface configuration command. To restore the default condition, use the **no** form of this command.

```
isdn negotiate-bchan [resend-setup]
```

```
no isdn negotiate-bchan [resend-setup]
```

### Syntax Description

<b>resend-setup</b>	(Optional) Supports NET5 and NI2 PRI switches only. Specifies that if the requested B channel is not available, the router resends a setup message requesting a different B channel.
---------------------	--

## isdn not-end-to-end

To override the speed that the network reports it will use to deliver the call data, use the **isdn not-end-to-end** interface configuration command. To disable the configured end-to-end speed, use the **no** form of this command.

```
isdn not-end-to-end {56 | 64}
```

```
no isdn not-end-to-end
```

### Syntax Description

<b>56</b>	Answers all voice calls at 56 kbps.
<b>64</b>	Answers all voice calls at 64 kbps.

## isdn nsf-service

To configure Network Specific Facilities (NSF) on an ISDN PRI for outgoing calls configured as voice calls, use the **isdn nsf-service** interface configuration command. To remove NSF on an ISDN PRI, use the **no** form of this command.

```
isdn nsf-service {megacom | sdn}
```

```
no isdn nsf-service {megacom | sdn}
```

### Syntax Description

<b>megacom</b>	Dial voice calls using AT&T Megacom NSF.
<b>sdn</b>	Dial voice calls using AT&T SDN NSF.

## isdn outgoing-voice

To set information transfer capability on outgoing calls for all switch types, use the **isdn outgoing-voice** interface configuration command. To revert to the default state, use the **no** form of this command.

```
isdn outgoing-voice {info-transfer-capability {3.1kHz-audio | speech}}
```

```
no isdn outgoing-voice
```

### Syntax Description

<b>info-transfer-capability</b>	Specifies information transfer capability for voice calls.
<b>3.1kHz-audio</b>	Sets capability to 3.1 kHz audio.
<b>speech</b>	Sets capability to speech.

## isdn overlap-receiving

To specify if the ISDN interface does Overlap Receiving, use the **isdn overlap-receiving** interface configuration command. To remove this capability, use the **no** form of this command.

```
isdn overlap-receiving
```

```
no isdn overlap-receiving
```

### Syntax Description

This command has no arguments or keywords.

## isdn piafs-enabled

To enable the PRI to take PIAFS (Personal Handyphone Internet Access Forum Standard) calls on MICA modems, use the **isdn piafs-enabled** interface configuration command. To disable the function, use the **no** form of this command.

**isdn piafs-enabled**

**no isdn piafs-enabled**

---

**Syntax Description** This command has no arguments or keywords.

## isdn point-to-point-setup

To configure the ISDN port to send SETUP messages on the static TEI, use the **isdn point-to-point-setup** interface configuration command. To restore the default, use the **no** form of this command.

**isdn point-to-point-setup**

**no isdn point-to-point-setup**

---

**Syntax Description** This command has no arguments or keywords.

## isdn protocol-emulate

To configure the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality, use the **isdn protocol-emulate** interface configuration command. To restore the default (user), use the **no** form of this command.

**isdn protocol-emulate** {user | network}

**no isdn protocol-emulate**

---

<b>Syntax Description</b>	<b>user</b>	Layer 2 and Layer 3 port protocol operation as TE (port functions as QSIG slave).
	<b>network</b>	Layer 2 and Layer 3 port protocol operation as NT (port functions as QSIG master).

---

## isdn rlm-group

To specify the RLM group number that ISDN will start using, use the **isdn rlm-group** interface configuration command. To disable this function, use the **no** form of this command.

**isdn rlm-group** *number*

**no isdn rlm-group** *number*

---

**Syntax Description**

<i>number</i>	Number of the RLM group, from 0 to 5.
---------------	---------------------------------------

---

## isdn send-alerting

To specify that an Alerting message be sent before a Connect message when making ISDN calls, use the **isdn send-alerting** interface configuration command. To disable the Alerting information element, use the **no** form of this command.

**isdn send-alerting**

**no isdn send-alerting**

---

**Syntax Description**

This command has no arguments or keywords.

## isdn sending-complete

To specify that the Sending Complete information element (IE) is included in the outgoing Setup message, use the **isdn sending-complete** interface configuration command. To disable the Sending Complete information element, use the **no** form of this command.

**isdn sending-complete**

**no isdn sending-complete**

---

**Syntax Description**

This command has no arguments or keywords.

## isdn service

To take an individual B channel or an entire PRI interface out of service or set it to a different channel service state that is passed to a time-division multiplexing (TDM) switch at the Public Switched Telephone Network (PSTN), use the **isdn service** command in interface configuration mode. To remove the configuration, use the **no** form of the command.

```
isdn service [dsl number | nfas-int number] b_channel number state {0 | 1 | 2}
```

```
no isdn service
```

Syntax Description	
<b>dsl number</b>	(Optional) Digital subscriber loop number; displayed with the <b>show isdn status</b> command. DSL numbers range from 0 to 31.
<b>nfas-int number</b>	(Optional) The Non-Facility Associated Signalling (NFAS) member interface number that has B channel(s) to which you want to do maintenance.
<b>b_channel number</b>	B channel or range of B channels to be set with the passed-in state value. Specifying <i>number</i> as 0 sets the entire PRI interface to a specified state value. B channel numbers range from 0 to 31 or 0 for the complete interface.
<b>state</b> {0   1   2}	Desired channel service state to be set on the channels. The following channel service state values are supported: <ul style="list-style-type: none"> <li><b>0</b>—In service. Restore a channel or complete interface to service.</li> <li><b>1</b>—Maintenance. “Soft busy.”</li> <li><b>2</b>—Out of service. Immediately take a channel(s) out of service and drop any active calls.</li> </ul>

## isdn snmp busyout b-channel

To enable PRI B channels to be busied out via SNMP, use the **isdn snmp busyout b-channel** interface configuration command. To prevent B channels from being busied out via SNMP, use the **no** form of this command.

```
isdn snmp busyout b-channel
```

```
no isdn snmp busyout b-channel
```

Syntax Description	
	This command has no keywords or arguments.

## isdn spid1, isdn spid2

To associate up to three ISDN local directory numbers (LDNs) provided by your telephone service provider to the first service profile identifier (SPID), use the **isdn spid1** interface configuration command. To disable the specified SPID and prevent access to the switch, use the **no** form of this command.

```
isdn spid1 spid-number ldn [ldn] [ldn]
```

```
no isdn spid1 spid-number ldn [ldn] [ldn]
```

To associate up to three ISDN LDNs provided by your telephone service provider to the second service SPID, use the **isdn spid2** interface configuration command. To disable the specified SPID and prevent access to the switch, use the **no** form of this command.

```
isdn spid2 spid-number ldn [ldn] [ldn]
```

```
no isdn spid2 spid-number ldn [ldn] [ldn]
```

### Syntax Description

<i>spid-number</i>	Number identifying the service to which you have subscribed. This value is assigned by the ISDN service provider and is usually a 10-digit telephone number with additional digits such as 40855522220101.
<i>ldn</i>	(Optional) ISDN LDN, which is a 7-digit number assigned by the service provider. You can optionally specify a second and third LDN.

## isdn switch-type (BRI)

To specify the central office switch type on the ISDN interface, use the **isdn switch-type** global or interface configuration command. To remove an ISDN switch type, use the **no** form of this command.

```
isdn switch-type switch-type
```

```
no isdn switch-type switch-type
```

### Syntax Description

<i>switch-type</i>	ISDN service provider switch type. Table 40 in lists the supported switch types.
--------------------	--

**Table 40** ISDN Service Provider BRI Switch Types

Keywords by Area	Switch Type
<b>Voice/PBX Systems</b>	
<b>basic-qsig</b>	PINX (PBX) switches with QSIG signalling per Q.931
<b>Australia , Europe, UK</b>	
<b>basic-ts013</b>	Australian BRI (TS013) switch
<b>basic-1tr6</b>	German 1TR6 ISDN switch

Table 40 ISDN Service Provider BRI Switch Types (continued)

Keywords by Area	Switch Type
<b>basic-net3</b>	NET3 ISDN and New Zealand NET3 switches (covers the Euro-ISDN E-DSS1 signalling system and is ETSI-compliant)
<b>vn3</b>	French ISDN BRI switches
<b>Japan</b>	
<b>ntt</b>	Japanese NTT ISDN switches
<b>North America</b>	
<b>basic-5ess</b>	Lucent (AT&T) basic rate 5ESS switch
<b>basic-dms100</b>	Northern Telecom DMS-100 basic rate switch
<b>basic-ni</b>	National ISDN switches
<b>All users</b>	
<b>none</b>	No switch defined

## isdn switch-type (PRI)

To specify the central office switch type on the ISDN interface, or to configure the Cisco MC3810 PRI interface to support QSIG signalling, use the **isdn switch-type** global and interface configuration command. To disable the switch or QSIG signalling on the ISDN interface, use the **no** form of this command.

**isdn switch-type** *switch-type*

**no isdn switch-type** *switch-type*

### Syntax Description

*switch-type* Service provider switch type; see Table 41 for a list of supported switches.

Table 41 ISDN Service Provider PRI Switch Types

Keywords by Area	Switch Type
<b>Voice/PBX Systems</b>	
<b>primary-qsig</b>	Supports QSIG signaling per Q.931. Network side functionality is assigned with the <b>isdn protocol-emulate</b> command.
<b>Australia and Europe</b>	
<b>primary-net5</b>	European, New Zealand and Asia ISDN PRI switches (covers the Euro-ISDN E-DSS1 signalling system and is ETSI-compliant).
<b>primary-ts014</b>	Australia PRI switch.
<b>Japan</b>	
<b>primary-ntt</b>	Japanese ISDN PRI switch.
<b>North America</b>	
<b>primary-4ess</b>	AT&T 4ESS switch type for the United States.

**Table 41 ISDN Service Provider PRI Switch Types (continued)**

<b>primary-5ess</b>	AT&T 5ESS switch type for the United States.
<b>primary-dms100</b>	NT DMS-100 switch type for the United States.
<b>primary-ni</b>	National ISDN switch type.
<b>All users</b>	
<b>none</b>	No switch defined.

## isdn t306

To set a timer for disconnect messages received by the router, use the **isdn t306** interface configuration command. To restore the default value, use the **default** or **no** form of this command.

**isdn t306** *msecs*

**default isdn t306**

**no isdn t306**

### Syntax Description

<i>msecs</i>	Number of milliseconds that the router waits before disconnecting a call after it receives a disconnect message with a progress indicator of 8. Values are 1 through 400,000 ms.
--------------	--

## isdn t310

To set a timer for the Call Proceeding state, use the **isdn t310** interface configuration command. To restore the default value, use the **no** form of this command.

**isdn t310** *msecs*

**no isdn t310**

### Syntax Description

<i>msecs</i>	Number of milliseconds that the router waits before disconnecting a call after receiving a Call Proceeding message. Values are 1 through 400,000 ms.
--------------	--

## isdn tei-negotiation

To configure when Layer 2 becomes active and ISDN terminal endpoint identifier (TEI) negotiation occurs, use the **isdn tei-negotiation** interface configuration and global configuration command. To remove TEI negotiation from an interface, use the **no** form of this command.

**isdn tei-negotiation** [**first-call** | **powerup**]

**no isdn tei-negotiation**

Syntax Description		
<b>first-call</b>	(Optional) ISDN TEI negotiation should occur when the first ISDN call is placed or received.	
<b>powerup</b>	(Optional) ISDN TEI negotiation should occur when the router is powered on.	

## isdn transfer-code

To activate call transferring, use the **isdn transfer-code** interface configuration command. To disable call transferring, use the **no** form of this command.

**isdn transfer-code** *range*

**no isdn transfer-code**

Syntax Description	<i>range</i>	Number from 0 to 999 (ISDN transfer code).
--------------------	--------------	--

## isdn twait-disable

To delay a National ISDN BRI switch a random time before activating the Layer 2 interface when the switch starts up, use the **isdn twait-disable** interface configuration command.

**isdn twait-disable**

**no isdn twait-disable**

Syntax Description	This command has no arguments or keywords.
--------------------	--

## isdn voice-priority

To control the priority of data and voice calls for the telephones, fax machines, and modems connected to the router telephone ports, use the **isdn voice-priority** interface configuration command. To disable a specified ISDN voice priority setting and to use the default setting, use the **no** form of this command.

**isdn voice-priority** *local-directory-number* {**in** | **out**} {**always** | **conditional** | **off**}

**no isdn voice-priority** *local-directory-number*

Syntax Description	<i>local-directory-number</i>	Local ISDN directory number assigned by your telephone service provider.
<b>in</b>		Incoming voice call.
<b>out</b>		Outgoing voice call.
<b>always</b>		Always bump a data call for a voice call.
<b>conditional</b>		Bump a data call only if there is more than one call to the same destination.
<b>off</b>		Never bump a data call for a voice call.

## isdn x25 dchannel

To create a configurable interface for X.25 traffic over the ISDN D channel, use the **isdn x25 dchannel** interface configuration command. To remove the interface, use the **no** form of this command.

**isdn x25 dchannel**

**no isdn x25 dchannel**

---

**Syntax Description** This command has no arguments or keywords.

## isdn x25 static-tei

To configure a static ISDN Layer 2 terminal endpoint identifier (TEI) for X.25 over the ISDN D channel, use the **isdn x25 static-tei** interface configuration command. Use the **no** form of this command if dynamic TEIs will be used on the interface that is to carry X.25 traffic over the D channel.

**isdn x25 static-tei** *tei-number*

**no isdn x25 static-tei** *tei-number*

---

**Syntax Description** *tei-number* Terminal endpoint identifier, in the range 0 to 63.

---

## l2f ignore-mid-sequence

To ignore multiplex ID (MID) sequence numbers for sessions in an Layer 2 Forwarding (L2F) tunnel, use the **l2f ignore-mid-sequence** VPDN group configuration command. To remove the ability to ignore MID sequencing, use the **no** form of this command.

**l2f ignore-mid-sequence**

**no l2f ignore-mid-sequence**

---

**Syntax Description** This command has no arguments or keywords.

## l2tp drop out-of-order

To instruct L2TP access concentrator (LAC) or L2TP Network Server (LNS) using Layer 2 Tunneling Protocol (L2TP) to drop packets that are received out of order, use the **l2tp drop out-of-order** VPDN group configuration command. To disable dropping of out-of-sequence packets, use the **no** form of this command.

**l2tp drop out-of-order**

**no l2tp drop out-of-order**

---

**Syntax Description** This command has no arguments or keywords.

## l2tp flow-control backoff-queuesize

To define the maximum number of packets that can be queued locally for a session when a peer's receive window is full, use the **l2tp flow-control backoff-queuesize** VPDN group configuration command. To change the value of the queue size, simply re-enter the command with the new queue size value. To remove a manually configured flow-control backoff value, use the **no** form of this command.

**l2tp flow-control backoff-queuesize** *queuesize*

**no l2tp flow-control backoff-queuesize** *queuesize*

---

<b>Syntax Description</b>	<i>queuesize</i>	Queue size limit on a LAC or LNS so that when the remote peer receive window is full, the LAC or LNS delays sending additional packets.
---------------------------	------------------	---

---

## l2tp flow-control maximum-ato

To define the maximum adaptive timeout for congestion control, use the **l2tp flow-control maximum-ato** VPDN group configuration command. To reset the timeout to a new value, simply reenter the command with the new value. To remove a manually configured timeout value, use the **no** form of this command.

**l2tp flow-control maximum-ato** *milliseconds*

**no l2tp flow-control maximum-ato** *milliseconds*

---

<b>Syntax Description</b>	<i>milliseconds</i>	Wait time period, in milliseconds, before the LAC or LNS probes its remote peer receive-window to resume sending packets.
---------------------------	---------------------	---

---

## I2tp flow-control receive-window

To define the receive window on a LAC or Layer 2 Tunneling Protocol Network Server (LNS) and enable either device to send sequence numbers, use the **i2tp flow-control receive-window** VPDN group configuration command. To remove a flow-control receive-window value and disable sequencing, use the **no** form of this command.

**i2tp flow-control receive-window** *window-size*

**no i2tp flow-control receive-window** *window-size*

---

<b>Syntax Description</b>	<i>window-size</i> The number of packets that can be received by the remote end device before backoff queuing occurs.
---------------------------	---

---

## I2tp flow-control static-rtt

To define a static round-trip time for congestion control, use the **i2tp flow-control static-rtt** VPDN group configuration command. To apply a different value, simply reenter the command with the new value. To disable a static round-trip time, use the **no** form of this command.

**i2tp flow-control static-rtt** *round-trip-time*

**no i2tp flow-control static-rtt** *round-trip-time*

---

<b>Syntax Description</b>	<i>round-trip-time</i> Static round-trip time in milliseconds.
---------------------------	--

---

## I2tp hidden

To enable Layer 2 Tunneling Protocol (L2TP) attribute-value (AV) pair hiding, which encrypts the AV pair “value,” use the **i2tp hidden** VPDN group configuration command. To disable L2TP AV pair value hiding, use the **no** form of this command.

**i2tp hidden**

**no i2tp hidden**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## l2tp ip tos reflect

To configure a Virtual Private Dialup Network (VPDN) group to preserve the ToS field of L2TP-tunneled IP packets, use the **l2tp ip tos reflect** VPDN group configuration command. To specify a ToS field of zero for tunneled packets, use the **no** form of this command.

**l2tp ip tos reflect**

**no l2tp ip tos reflect**

---

**Syntax Description** This command has no arguments or keywords.

## l2tp ip udp checksum

To enable IP User Data Protocol (UDP) checksums on Layer 2 Tunneling Protocol (L2TP) payload packets, use the **l2tp ip udp checksum** VPDN group configuration command. To disable IP UDP checksums, use the **no** form of this command.

**l2tp ip udp checksum**

**no l2tp ip udp checksum**

---

**Syntax Description** This command has no arguments or keywords.

## l2tp offset

To enable the offset field in Layer 2 Tunneling Protocol (L2TP) payload packets, use the **l2tp offset** VPDN group configuration command. To disable the offset field, use the **no** form of this command.

**l2tp offset**

**no l2tp offset**

---

**Syntax Description** This command has no arguments or keywords.

## I2tp tunnel authentication

To enable Layer 2 Tunneling Protocol (L2TP) tunnel authentication, use the **i2tp tunnel authentication** VPDN group configuration command. To disable L2TP tunnel authentication, use the **no** form of this command.

**i2tp tunnel authentication**

**no i2tp tunnel authentication**

---

**Syntax Description** This command has no arguments or keywords.

## I2tp tunnel hello

To set the number of seconds between sending hello keepalive packets for a Layer 2 Tunneling Protocol (L2TP) tunnel, use the **i2tp tunnel hello** VPDN group configuration command. To change the tunnel hello value, simply reenter the command with the new value. To disable the sending of hello keepalive packets, use the **no** form of this command.

**i2tp tunnel hello** *hello-interval*

**no i2tp tunnel hello** *hello-interval*

---

**Syntax Description** *hello-interval* The interval, in seconds, that the LAC and LNS wait before sending the next L2TP tunnel keepalive packet.

---

## I2tp tunnel password

To set the password that the router will use to authenticate the tunnel, use the **i2tp tunnel password** VPDN group configuration command. To remove a previously configured password, use the **no** form of this command.

**i2tp tunnel password** *password*

**no i2tp tunnel password** *password*

---

**Syntax Description** *password* String that the router uses for tunnel authentication.

---

## lcp renegotiation

To allow the L2TP Network Server (LNS) to renegotiate the Link Control Protocol (LCP) on dial-in calls, using Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F), use the **lcp renegotiation** VPDN group configuration command. To remove LCP renegotiation, use the **no** form of this command.

**lcp renegotiation** { *always* | *on-mismatch* }

**no lcp renegotiation**

Syntax Description		
	<b>always</b>	Always renegotiate PPP LCP at the LNS.
	<b>on-mismatch</b>	Renegotiates PPP LCP at the LNS only in the event of an LCP mismatch between the LAC and LNS.

## limit base-size

To define the base number of simultaneous connections that can be done in a single customer or virtual private dialup network (VPDN) profile, use the **limit base-size** customer profile configuration or VPDN profile configuration command. To remove the limitation, use the **no** form of this command.

**limit base-size** { *number* | *all* }

**no limit base-size** { *number* | *all* }

Syntax Description		
	<i>number</i>	Maximum number of simultaneous connections or sessions that can be used in a specified customer or VPDN profile.
	<b>all</b>	Accepts all calls. Use this command if you do not want to limit or apply overflow session counting to a customer or VPDN profile.

## limit overflow-size

To define the number of overflow calls granted to one customer or virtual private dialup network (VPDN) profile, use the **limit overflow-size** customer profile configuration or VPDN profile configuration command. To remove the overflow configuration, use the **no** form of this command.

**limit overflow-size** { *number* | *all* }

**no limit overflow-size** { *number* | *all* }

Syntax Description		
	<i>number</i>	Number of overflow calls.
	<b>all</b>	Allows an unlimited number of overflow calls.

## line

To identify a specific line for configuration and begin the line configuration collection mode, use the **line** global configuration command.

```
line [aux | console | tty | vty] line-number [ending-line-number]
```

### Syntax Description

<b>aux</b>	(Optional) Auxiliary EIA/TIA-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.
<b>console</b>	(Optional) Console terminal line. The console port is DCE.
<b>tty</b>	(Optional) Standard asynchronous line.
<b>vty</b>	(Optional) Virtual terminal for remote console access.
<i>line-number</i>	Relative number of the terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified. Numbering begins with zero.
<i>ending-line-number</i>	(Optional) Relative number of the last line in a contiguous group that you want to configure. If you omit the keyword, then <i>line-number</i> and <i>ending-line-number</i> are absolute rather than relative line numbers.

## line-power

To configure a BRI port to supply line power to the terminal equipment (TE), use the **line-power** interface configuration command. To disable the line power supply, use the **no** form of this command.

```
line-power
```

```
no line-power
```

### Syntax Description

This command has no arguments or keywords.

## link (RLM)

To enable a Redundant Link Manager (RLM) link, use the **link** RLM configuration command. To disable this function, use the **no** form of this command.

```
link {hostname name | address ip-address} source interface weight number
```

```
no link {hostname name | address ip-address} source interface weight number
```

Syntax Description		
<b>hostname</b> <i>name</i>		RLM host name. If host name is used, RLM will look up the DNS server periodically for the host name configured until lookup is successful or the configuration is removed.
<b>address</b> <i>ip-address</i>		IP address of the link.
<b>source</b> <i>interface</i>		Loopback interface source. We recommend you use the loopback interface as the source, so that it is independent of the hardware condition. Also, the source interface should be different in every link to avoid falling back to the same routing path. If you intend to use the same routing path for the failover, a single link is sufficient to implement it.
<b>weight</b> <i>number</i>		Priority set as a weight factor. The higher the weighting number, the higher priority it gets to become the active link. If all entries have the same weighting, all links will be treated equally. There is no preference among servers according to the assumption that only one server will accept the connection requests at any given time. Otherwise, the preference will extend across all servers.

## loadsharing

To configure endpoints for load sharing, use the **loadsharing** VPDN group configuration command. To remove this function, use the **no** form of this command.

**loadsharing ip** *ip-address* [**limit** *number*]

**no loadsharing ip** *ip-address* [**limit** *number*]

Syntax Description		
<b>ip</b> <i>ip-address</i>		IP address of the HGW/LNS at the other end of the tunnel. This is the IP endpoint at the end of the tunnel, which is a HGW/LNS router.
<b>limit</b> <i>number</i>		(Optional) Limits sessions per load share. The limit has a range from 0 to 32,767 sessions. The default is no limit set.

## local name

To specify a local host name that the tunnel will use to identify itself, use the **local name** global configuration command. To remove a local name, use the **no** form of this command.

**local name** *name*

**no local name** *name*

Syntax Description		
<i>name</i>		Local host name of the tunnel.

## loopback (controller)

To loop an entire E1 line (including all channel groups defined on the controller) toward the line and back toward the router or access server, use the **loopback** controller configuration command. To remove the loop, use the **no** form of this command.

**loopback**

**no loopback**

---

**Syntax Description** This command has no arguments or keywords.

## loopback local (controller)

To loop an entire T1 line (including all channel groups defined on the controller) toward the line and the router or access server, use the **loopback local** controller configuration command. To remove the loop, use the **no** form of this command.

**loopback local**

**no loopback local**

---

**Syntax Description** This command has no arguments or keywords.

## loopback local (interface)

To loop a channelized T1 or channelized E1 channel group, use the **loopback local** interface configuration command. To remove the loop, use the **no** form of this command.

**loopback local**

**no loopback local**

---

**Syntax Description** This command has no arguments or keywords.

## loopback remote (controller)

To loop packets from a MultiChannel Interface Processor (MIP) through the CSU/DSU, over a dedicated T1 link, to the remote CSU at the single destination for this T1 link and back, use the **loopback remote** controller configuration command. To remove the loop, use the **no** form of this command.

**loopback remote**

**no loopback remote**

---

**Syntax Description** This command has no arguments or keywords.

## map-class dialer

To define a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback, use the **map-class dialer** global configuration command.

**map-class dialer** *class-name*

---

**Syntax Description**

<i>class-name</i>	Unique class identifier.
-------------------	--------------------------

---

## member

To alter the configuration of an asynchronous interface that is a member of a group, use the **member** interface configuration command. To restore defaults set at the group master interface, use the **no** form of this command.

**member** *number interface-command*

**no member** *number interface-command*

---

**Syntax Description**

<i>number</i>	Number of the asynchronous interface to be altered.
<i>interface-command</i>	One or more of the following commands entered for this specific interface: <ul style="list-style-type: none"> <li>• <b>peer default ip address</b></li> <li>• <b>description</b></li> </ul>

---

## member (dial peer cor list)

To add a member to a dial peer class of restrictions (COR) list, use the **member** dial peer cor list configuration command. To remove a member from a list, use the **no** form of this command.

**member** *class-name*

**no member** *class-name*

<b>Syntax Description</b>	<i>class-name</i>	Class name previously defined in dial peer COR custom configuration mode by using of the <b>name</b> command.
---------------------------	-------------------	---

## modem answer-timeout

To set the amount of time that the Cisco IOS software waits for the Clear to Send (CTS) signal after raising the data terminal ready (DTR) signal in response to RING, use the **modem answer-timeout** line configuration command. To revert to the default value, use the **no** form of this command.

**modem answer-timeout** *seconds*

**no modem answer-timeout**

<b>Syntax Description</b>	<i>seconds</i>	Timeout interval in seconds.
---------------------------	----------------	------------------------------

## modem at-mode

To open a directly connected session and enter AT command mode, which is used for sending AT commands to Microcom manageable modems, use the **modem at-mode EXEC** command.

**modem at-mode** *slot/port*

<b>Syntax Description</b>	<i>slot/port</i>	Slot and modem port number. (Include the forward slash (/) when entering this variable.)
---------------------------	------------------	--

## modem at-mode-permit

To permit a Microcom modem to accept a directly connected session, use the **modem at-mode-permit** line configuration command. To disable permission for modems to accept a direct connection, use the **no** form of this command.

**modem at-mode-permit**

**no modem at-mode-permit**

---

**Syntax Description** This command has no arguments or keywords.

## modem autoconfigure discovery

To configure a line to discover what kind of modem is connected to the router and to configure that modem automatically, use the **modem autoconfigure discovery** line configuration command. To disable this feature, use the **no** form of this command.

**modem autoconfigure discovery**

**no modem autoconfigure discovery**

---

**Syntax Description** This command has no arguments or keywords.

## modem autoconfigure type

To direct a line to attempt to configure the attached modem using the entry for the *modem-name* argument, use the **modem autoconfigure type** line configuration command. To disable this feature, use the **no** form of this command.

**modem autoconfigure type** *modem-name*

**no modem autoconfigure type**

---

**Syntax Description**

<i>modem-name</i>	Name of the modem (such as Codex_3260).
-------------------	---

---

## modem autotest

To automatically and periodically perform a modem diagnostics test for modems inside the access server or router, use the **modem autotest** global configuration command. To disable or turn off the modem autotest service, use the **no** form of this command.

**modem autotest** {*error threshold* | **minimum** *modem* | **time** *hh:mm* [*interval*]}

**no modem autotest**

Syntax Description		
<b>error threshold</b>		Maximum modem error threshold. When the system detects this many errors with the modems, the modem diagnostics test is automatically triggered. Specify a threshold count between 3 and 50.
<b>minimum modem</b>		Minimum number of modems that will remain untested and available to accept calls during each test cycle. You can specify between 5 and 48 modems. The default is 6 modems.
<b>time hh:mm</b>		Time when you want the modem autotest to begin. You must use the military time convention and a required colon (:) between the hours and minutes variables for this feature. For example, 1:30 a.m. is issued as 01:30.
<b>interval</b>		(Optional) Long-range time variable used to set the modem autotest more than one day in advance. The range of hours is between 1 hour and 168 hours. For example, if you want to run the test once per week, issue 168. There are 168 hours in one week.

## modem bad

To remove an integrated modem from service and indicate it as suspected or proven to be inoperable, use the **modem bad** line configuration command. To restore a modem to service, use the **no** form of this command.

**modem bad**

**no modem bad**

**Syntax Description** This command has no arguments or keywords.

## modem buffer-size

To configure the size of the history event queue buffer for integrated modems installed in an access server or router, use the **modem buffer-size** global configuration command.

**modem buffer-size number**

**Syntax Description** *number* Defined number of modem events that each manageable modem is able to store.

## modem busyout

To gracefully disable a modem from dialing or answering calls, use the **modem busyout** line configuration command. To reenable a modem, use the **no** form of this command.

**modem busyout**

**no modem busyout**

**Syntax Description** This command has no arguments or keywords.

## modem busyout-threshold

To define a threshold to maintain a balance between the number of DS0s and modems, use the **modem busyout-threshold** global configuration command. To remove the threshold, use the **no** form of this command.

### Cisco AS5350 and AS5400 Access Servers Only

**modem busyout-threshold** *threshold-number*

**no modem busyout-threshold** *threshold-number*



#### Note

This command is the same as the **ds0 busyout-threshold** command for the Cisco AS5300 and AS5800 access servers.

Syntax Description	<i>threshold-number</i>	Number of modems that are free when the router should enforce the stipulation that the number of free DS0 lines is less than or equal to the number of modems.
--------------------	-------------------------	--

## modem callin

To support dial-in modems that use the data terminal ready (DTR) signal to control the off-hook status of the modem, use the **modem callin** line configuration command. To disable this feature, use the **no** form of this command.

**modem callin**

**no modem callin**

Syntax Description	This command has no arguments or keywords.
--------------------	--

## modem callout

To configure a line for reverse connections, use the **modem callout** line configuration command. To disable this feature, use the **no** form of this command.

**modem callout**

**no modem callout**

Syntax Description	This command has no arguments or keywords.
--------------------	--

## modem country mica

To configure the modem country code for a bank of MICA technologies modems, use the **modem country mica** global configuration command. To remove a country code from service, use the **no** form of this command.

**modem country mica** *country*

**no modem country mica** *country*

### Syntax Description

*country* Country name. See Table 42 for a list of the supported country name arguments.

**Table 42** MICA Country Names

australia

austria

belgium

china

cyprus

czech-republic (Czech/Slovak Republic)

denmark

e1-default (Default E1, A Law)

finland

france

germany

hong-kong

india

ireland

israel

italy

japan

malaysia

netherlands

new-zealand

norway

poland

portugal

russia

singapore

south-africa

**Table 42** MICA Country Names (continued)

spain
sweden
switzerland
t1-default (Defaults T1, u Law)
taiwan
thailand
turkey
united-kingdom
usa

## modem country microcom\_hdms

To configure the modem country code for a bank of Microcom modems, use the **modem country microcom\_hdms** global configuration command. To remove a country code from service, use the **no** form of this command.

**modem country microcom\_hdms** *country*

**no modem country microcom\_hdms** *country*

### Syntax Description

*country* Country name. See Table 43 for a list of the supported country name arguments.

**Table 43** Microcom Country Names

argentina
australia
austria
belgium
brazil
canada
chile
china
columbia
czech-republic (Czech/Slovak Republic)
denmark
europa
finland
france
germany

**Table 43** *Microcom Country Names (continued)*

greece
hong-kong
hungary
india
indonesia
finland
israel
italy
japan
korea
malaysia
mexico
netherlands
norway
peru
philippines
poland
portugal
saudi-arabia
singapore
south-africa
spain
sweden
switzerland
taiwan
thailand
united-kingdom
usa

## modem cts-required

The **modem cts-required** command is replaced by the **modem printer** command. See the description of the **modem printer** command for more information.

## modem dialin

To configure a line to enable a modem attached to the router to accept incoming calls only, use the **modem dialin** line configuration command. To disable this feature, use the **no** form of this command.

**modem dialin**

**no modem dialin**

**Syntax Description** This command has no arguments or keywords.

## modem dialout controller

To specify a particular T1 or E1 controller through which to dialout, use the **modem dialout controller** line configuration mode command. To disable, use the **no** form of this command.

**modem dialout controller** {**e1** | **t1**} {*number*}

**no modem dialout controller**

<b>Syntax Description</b>	<b>e1</b>	Wide-area digital transmission scheme used predominantly in Europe.
	<b>t1</b>	Wide-area digital carrier facility.
	<i>number</i>	List of controllers through which to dialout. The range is from 0 to 7. List the controllers individually (1,2,3).

## modem dtr-active

To configure a line to leave data terminal ready (DTR) signals low, unless the line has an active incoming connection or an EXEC process, use the **modem dtr-active** line configuration command. To disable this feature, use the **no** form of this command.

**modem dtr-active**

**no modem dtr-active**

**Syntax Description** This command has no arguments or keywords.

## modem hold-reset

To reset and isolate integrated modems for extensive troubleshooting, use the **modem hold-reset** line configuration command. To restart a modem, use the **no** form of this command.

**modem hold-reset**

**no modem hold-reset**

---

**Syntax Description** This command has no arguments or keywords.

## modem host

To configure a line for reverse connections where hardware flow control is also required, use the **modem host** line configuration command. To disable the line modem control for reverse connections, use the **no** form of this command.

**modem host**

**no modem host**

---

**Syntax Description** This command has no arguments or keywords.

## modem inout

To configure a line for both incoming and outgoing calls, use the **modem inout** line configuration command. To disable the line, use the **no** form of this command.

**modem inout**

**no modem inout**

---

**Syntax Description** This command has no arguments or keywords.

## modem link-info poll time

To set the polling interval at which link statistics are retrieved from the MICA modem, use the **modem link-info poll time** global configuration command. To return to the default condition, use the **no** form of this command.

**modem link-info poll time** *seconds*

**no modem link-info poll time** *seconds*

### Syntax Description

<i>seconds</i>	Number of seconds between polling intervals. The valid range is 10 to 65,535.
----------------	---

## modem min-speed max-speed

To configure various modem-service parameters, use the **modem min-speed max-speed** service profile configuration command. To remove modem parameters, use the **no** form of this command.

**modem min-speed** {*speed* | **any**} **max-speed** {*speed* | **any** [**modulation value**]}

**no modem min-speed** {*speed* | **any**} **max-speed** {*speed* | **any** [**modulation value**]}

### Syntax Description

<i>speed</i>	Minimum and maximum bps rate for the modems, which can be between 300 and 56,000 bps. Must be in V.90 increments.
<b>any</b>	Any minimum or maximum speed.
<b>modulation value</b>	(Optional) Maximum negotiated speed. Replace the <i>value</i> argument with one of the following choices: <b>any</b> , <b>k56flex</b> , <b>v22bis</b> , <b>v34</b> , or <b>v90</b> .

## modem poll retry

To set the maximum number of polling attempts used to retrieve performance statistics from a modem installed in an access server or router, use the **modem poll retry** global configuration command.

**modem poll retry** *number*

### Syntax Description

<i>number</i>	Maximum number of polling attempts. The configuration range is from 0 to 10 attempts.
---------------	---

## modem poll time

To set the time interval between modem polls, which are used to periodically retrieve and report modem statistics, use the **modem poll time** global configuration command. To restore the 12-second default setting, use the **no** form of this command.

**modem poll time** *seconds*

**no modem poll time** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds between polls. The configuration range is from 2 to 120 seconds.
---------------------------	----------------	--

## modem printer

To configure a line to require a Data Set Ready (DSR) signal, use the **modem printer** line configuration command. To use Clear to Send (CTS) instead of DSR, use the **no** form of this command.

**modem printer**

**no modem printer**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## modem recovery action

To specify the modem recovery mode, use the **modem recovery action** global configuration command. To turn off this feature, use the **no** form of this command.

**modem recovery action** { **disable** | **download** | **none** }

**no modem recovery action**

<b>Syntax Description</b>	<b>disable</b>	Marks the modem bad.
	<b>download</b>	Recovers by firmware download. Sets the modem into a recovery pending state, thus, stopping the modem from accepting new calls.
	<b>none</b>	Does not try to recover. Ignores the recovery threshold and just keeps going.

## modem recovery maintenance

To specify the modem maintenance recovery behavior, use the **modem recovery maintenance** global configuration command. To turn off this behavior, use the **no** form of this command.

```
modem recovery maintenance {action {disable | drop-call | reschedule} | max-download
  number | schedule {immediate | pending} | time hh:mm | window minutes}
```

```
no modem recovery maintenance
```

### Syntax Description

<b>action</b>	Mode of recovery. The default is set to <b>reschedule</b> .
<b>disable</b>	Marks the modem bad. Marks the originally faulty modem as bad and returns all other modems back into service.
<b>drop-call</b>	Forces firmware download by dropping holding calls. This forces the recovery by dropping any active calls remaining on modems within the module.
<b>reschedule</b>	Reschedule firmware download to next maintenance time. Leaves the originally faulty modem as needing recovery and returns all other modems into service. Recovery will be attempted again on the following day. The default is set to reschedule.
<b>max-download</b> <i>number</i>	Maximum simultaneous recovery downloads. You must choose one number from 1 to 30. A range of values is not supported.
<b>schedule</b>	Scheduling method for modem recovery. Determines if the system should attempt module recovery as soon as a problem is found or wait for the maintenance window.
<b>immediate</b>	Immediately attempts module recovery.
<b>pending</b>	Delays recovery until maintenance time.
<b>time</b> <i>hh:mm</i>	Time of day for scheduled modem recovery. This is the actual time of day when the modem recovery maintenance process wakes up and starts recovering MICA technologies modems. The default time is 3:00 a.m.
<b>window</b> <i>minutes</i>	Amount of time for normal recovery to take place. This is the delay timer in minutes, which is from 0 to 360.

## modem recovery threshold

To specify the threshold, which starts the modem recovery process, use the **modem recovery threshold** global configuration command. To disable the threshold value, use the **no** form of this command.

```
modem recovery threshold number
```

```
no modem recovery threshold
```

### Syntax Description

<i>number</i>	Number of consecutive call attempts that fail to train up before the modem is deemed faulty. Choose from 1 to 1000.
---------------	---

## modem recovery-time

To set the maximum amount of time the call-switching module waits for a local modem to respond to a request before it is considered locked in a suspended state, use the **modem recovery-time** global configuration command. To set a 5-minute response time, which is the default setting, use the **no** form of this command.

**modem recovery-time** *minutes*

**no modem recovery-time**

---

<b>Syntax Description</b>	<i>minutes</i>	Maximum amount of time for which local modems wait for a response.
---------------------------	----------------	--

---

## modem ri-is-cd

The **modem ri-is-cd** command is replaced by the **modem dialin** command. See the description of the **modem dialin** command for more information.

## modem shutdown

To abruptly shut down an active or idle modem installed in an access server or router, use the **modem shutdown** line configuration command. To take the modem out of a shutdown state and place it back in service, use the **no** form of this command.

**modem shutdown**

**no modem shutdown**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## modem startup-test

To perform diagnostic testing on each integrated modem during the rebooting process, use the **modem startup-test** global configuration command. To disable startup testing, use the **no** form of this command.

**modem startup-test**

**no modem startup-test**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## modem status-poll

To poll for modem statistics through a modem's out-of-band feature, use the **modem status-poll** line configuration command. To disable status polling through the out-of-band feature for a specified modem, use the **no** form of this command.

**modem status-poll**

**no modem status-poll**

**Syntax Description** This command has no arguments or keywords.

## modemcap edit

To change a modem value that was returned from the **show modemcap** command, use the **modemcap edit** global configuration command.

**modemcap edit** *modem-name attribute at-command*

<b>Syntax Description</b>	<i>modem-name</i>	Name of the modem whose values are being edited.
	<i>attribute</i>	Modem capability, or attribute, as defined by the <b>show modemcap</b> command.
	<i>at-command</i>	The AT command equivalent (such as <b>&amp;F</b> ).

## modemcap entry

To store and compress information about the capability of a specified modem, use the **modemcap entry** global configuration command. To disable this feature, use the **no** form of this command.

**modemcap entry** *modem-type*

**no modemcap entry** *modem-type*

<b>Syntax Description</b>	<i>modem-type</i>	Type of supported modem as specified in Table 44.
---------------------------	-------------------	---

**Table 44 Modemcap Entries for Supported Modems**

Modemcap Name	Modem Type
<b>External Modems</b>	
<b>codex_3260</b>	Motorola Codex 3260
<b>default</b>	Generic "Hayes" interface
<b>global_village</b>	Global Village Teleport1
<b>hayes_optima</b>	Hayes Optima <sup>1</sup>

**Table 44** Modemcap Entries for Supported Modems (continued)

Modemcap Name	Modem Type
<b>nec_piafs</b>	NEC PIAFS TA
<b>nec_v34</b>	NEC V.34
<b>nec_v110</b>	NEC V.110 TA
<b>telebit_t3000</b>	Telebit T3000
<b>usr_courier</b>	U.S. Robotics Courier
<b>usr_sportster</b>	U.S. Robotics Sportster
<b>viva</b>	Viva (Rockwell ACF with MNP)
<b>Internal Modems</b>	
<b>cisco_v110</b>	Cisco (NEC) internal V.110 TA (AS 5200)
<b>mica</b>	Cisco MICA HMM/DMM digital
<b>microcom_hdms</b>	Microcom HDMS chassis
<b>microcom_mimic</b>	Cisco (Microcom) analog (NM-AM-2600/3600)
<b>microcom_server</b>	Cisco (Microcom) V.34/56K digital (AS 5300)
<b>nextport</b>	Cisco NextPort CSMV/6 digital

1. This built in modemcap is not recommended for use on an Optima because it sets the modem to automatic speed buffering. This disables error control and may result in poor performance. Instead, use modemcap **default**.

## modem-pool

To create a new modem pool or to specify an existing modem pool, use the **modem-pool** global configuration command. To delete a modem pool from the access server configuration, use the **no** form of this command.

**modem-pool** *name*

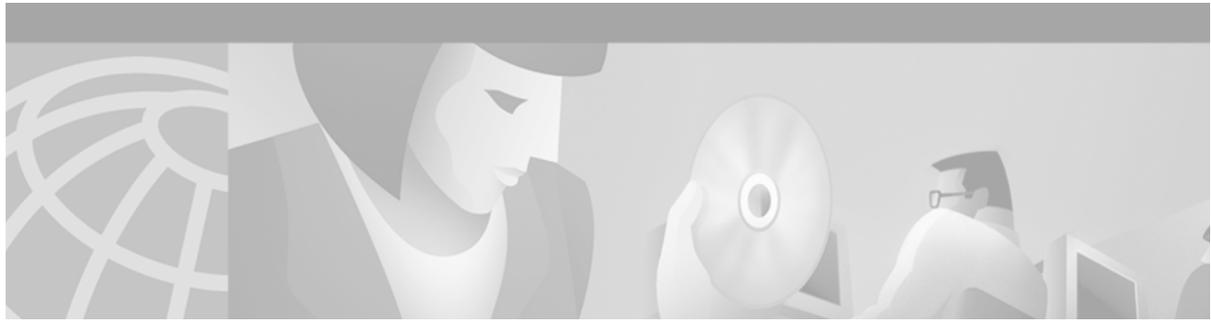
**no modem-pool** *name*

---

### Syntax Description

<i>name</i>	Name of a modem pool.
-------------	-----------------------

---



## Dial Technologies Commands: **multilink bundle-name** Through **shelf-id**

---

This chapter describes the function and syntax of the dial technologies commands: **multilink bundle-name** through **shelf-id**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Dial Technologies Command Reference*.

### **multilink bundle-name**

To select a method for naming multilink bundles, use the **multilink bundle-name** global configuration command. To remove the selection method, use the **no** form of this command.

```
multilink bundle-name { authenticated | endpoint | both }
```

```
no multilink bundle-name { authenticated | endpoint | both }
```

---

#### **Syntax Description**

<b>authenticated</b>	Authenticated name of the peer. This is the default.
<b>endpoint</b>	Endpoint discriminator of the peer.
<b>both</b>	Authenticated name and endpoint discriminator of the peer.

---

### **multilink-group**

The **multilink-group** command is replaced by the **ppp multilink group** command. See the description of the **ppp multilink group** command for more information.



#### **Note**

---

The command is still recognized and accepted by the Cisco IOS software. The **show running-config** and **write memory** commands will display and generate the original command in Cisco IOS Release 12.2.

---

## multilink virtual-template

To specify a virtual template from which the specified Multilink PPP (MLP) bundle interface can clone its interface parameters, use the **multilink virtual-template** global configuration command.

**multilink virtual-template** *number*

---

### Syntax Description

<i>number</i>	Number of virtual templates, and is an integer in the range 1 through the largest number of virtual templates the software image supports (typically 25).
---------------	---

---

## name (dial peer cor custom)

To specify the name for a custom class of restrictions (COR), use the **name** dial peer cor custom configuration command. To remove a previously named custom COR, use the **no** form of this command.

**name** *class-name*

**no name** *class-name*

---

### Syntax Description

<i>class-name</i>	Name that describes the specific COR.
-------------------	---------------------------------------

---

## netbios nbf

To enable the NetBIOS Frames Protocol (NBF) on an interface, use the **netbios nbf** interface configuration command. To disable NetBIOS Frames Protocol support on an interface, use the **no** form of this command.

**netbios nbf**

**no netbios nbf**

---

### Syntax Description

This command has no arguments or keywords.

## network-clock-priority

To specify the clock-recovery priority for the BRI voice ports in a BRI voice module (BVM), use the **network-clock-priority** interface configuration command. To restore the default (low) clock-recovery priority, use the **no** form of this command.

**network-clock-priority** {**low** | **high**}

**no network-clock-priority** {**low** | **high**}

Syntax Description		
	<b>low</b>	The BRI port is second priority to recover clock.
	<b>high</b>	The BRI port is first priority to recover clock.

## network-clock-select

To specify selection priority for the clock sources, use the **network-clock-select** global configuration command. To cancel the network clock selection, use the **no** form of this command.

**network-clock-select** *priority* {**serial 0** | **system** | **bvm** | *controller*}

**no network-clock-select** *priority* {**serial 0** | **system** | **bvm** | *controller*}

Syntax Description		
	<i>priority</i>	Selection priority for the clock source from 1 (highest) to 4 (lowest).
	<b>serial 0</b>	Clocking priority for serial interface 0.
	<b>system</b>	Clocking priority for the system clock.
	<b>bvm</b>	Clocking priority for the BRI voice module (BVM).
	<i>controller</i>	Clocking priority for either the trunk controller (T1/E1 0) or the digital voice module (T1/E1/ 1).

## number

To add a Calling Line Identification (CLID) or Dialed Number Identification Service (DNIS) number to a dialer group, use the **number** CLID or DNIS group configuration command followed by the specifying number. To remove a number from a group, use the **no** form of this command.

**number** *number*

**no number** *number*

Syntax Description		
	<i>number</i>	CLID or DNIS number, which can have up to 65 digits.

## permission (dial peer voice)

To specify whether incoming or outgoing calls are permitted on the defined dial peer, use the **permission** dial peer voice configuration command. To remove the specified permission, use the **no** form of this command.

**permission** { **orig** | **term** | **both** | **none** }

**no permission** { **orig** | **term** | **both** | **none** }

Syntax Description		
<b>orig</b>		This dial peer is permitted to originate calls. Thus, the access server can accept incoming calls from the dial peer.
<b>term</b>		This dial peer is permitted to terminate calls. Thus, the access server can send outgoing calls to the dial peer.
<b>both</b>		This dial peer is permitted to originate and terminate calls. Both incoming and outgoing calls are permitted.
<b>none</b>		No incoming or outgoing calls can be made to or from this dial peer.

## pool-member

To assign a request-dialout virtual private dialup network (VPDN) subgroup to a dialer pool, use the **pool-member** request-dialout configuration command. To remove the request-dialout VPDN subgroup from a dialer pool, use the **no** form of this command.

**pool-member** *pool-number*

**no pool-member** [*pool-number*]

Syntax Description	<i>pool-number</i>	Dialer pool that this VPDN group belongs to.

## pool-range

To assign a range of modems to a modem pool, use the **pool-range** modem-pool configuration command.

**pool-range** *number-number*

Syntax Description	<i>number-number</i>	Range of TTY lines, which correspond to ranges of modems or to a modem pool. A hyphen (-) is required between the two modem numbers. The range of modems you can choose from is equivalent to the number of modems in your access server that are not currently associated with another modem pool.

# port

To enter the port configuration mode, use the **port** global configuration command. To exit port configuration mode, use the **no** form of this command.

## Cisco AS5400 with NextPort DFC

```
port {slot | slot/port}
```

## Cisco AS5800 with Universal Port Card

```
port {shelfslot | shelfslot/port}
```

Syntax Description	slot	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	slot/port	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
	shelfslot	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	shelfslot/port	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

# port modem autotest

To automatically and periodically perform a modem diagnostics test for modems inside the access server or router, use the **port modem autotest** global configuration command. To disable or turn off the modem autotest service, use the **no** form of this command.

```
port modem autotest {error threshold | minimum modem | time hh:mm [interval]}
```

```
no port modem autotest
```

Syntax Description	error threshold	Maximum modem error threshold. When the system detects this many errors with the modems, the modem diagnostics test is automatically triggered. Specify a threshold count between 3 and 50.
	minimum modem	Minimum number of modems that will remain untested and available to accept calls during each test cycle. You can specify between 5 and 48 modems. The default is 6 modems on the Cisco AS5400. The range for the Cisco AS5800 is 73 to 756.
	time hh:mm	Time you want the modem autotest to begin. You must use the military time convention and a required colon (:) between the hours and minutes variables for this feature. For example, 1:30 a.m. is issued as 01:30.
	interval	(Optional) Long-range time variable used to set the modem autotest more than one day in advance. The range of hours is between 1 hour and 168 hours. For example, if you want to run the test once per week, issue 168. There are 168 hours in one week.

## ppp

To start an asynchronous connection using PPP, use the **ppp EXEC** command.

```
ppp [/default | {remote-ip-address | remote-name} [@tacacs-server]] [/routing]
```

Syntax Description		
<b>/default</b>	Makes a PPP connection when a default address has been configured.	
<i>remote-ip-address</i>	IP address of the client workstation or PC. This parameter can only be specified if the line is set for dynamic addresses using the <b>async address dynamic</b> line configuration command.	
<i>remote-name</i>	Name of the client workstation or PC. This parameter can be specified if the line is set for dynamic addresses using the <b>async address dynamic</b> line configuration command.	
<i>@tacacs-server</i>	(Optional) IP address or IP host name of the TACACS server to which the user's TACACS authentication request is sent.	
<b>/routing</b>	(Optional) Indicates that the remote system is a router and that routing messages should be exchanged over the link. The line must be configured for asynchronous routing using PPP encapsulation.	

## ppp bap call

To set PPP Bandwidth Allocation Protocol (BACP) call parameters, use the **ppp bap call** interface configuration command. To disable processing of a specific type of incoming connection, use the **no** form of this command.

```
ppp bap call {accept | request | timer seconds}
```

```
no ppp bap call {accept | request | timer}
```

Syntax Description		
<b>accept</b>	Peer initiates link addition. This is the default.	
<b>request</b>	Local side initiates link addition.	
<b>timer seconds</b>	Number of seconds to wait between call requests the router sends, in the range 2 to 120 seconds. No default value is set.	

## ppp bap callback

To enable PPP Bandwidth Allocation Protocol (BACP) callback and set callback parameters, use the **ppp bap callback** interface configuration command. To remove the PPP BACP callback configuration, use the **no** form of this command.

```
ppp bap callback {accept | request | timer seconds}
```

```
no ppp bap callback {accept | request | timer}
```

Syntax Description		
	<b>accept</b>	Local router initiates link addition upon peer notification.
	<b>request</b>	Local router requests that a peer initiate link addition.
	<b>timer</b> <i>seconds</i>	Number of seconds to wait between callback requests the router sends, in the range 2 to 120 seconds. Disabled by default.

## ppp bap drop

To set parameters for removing links from a multilink bundle, use the **ppp bap drop** interface configuration command. To disable a specific type of default processing, use the **no** form of this command.

```
ppp bap drop {accept | after-retries | request | timer seconds}
```

```
no ppp bap drop {accept | after-retries | request | timer}
```

Syntax Description		
	<b>accept</b>	Peer can initiate link removal. Enabled by default.
	<b>after-retries</b>	Local router can remove the link without Bandwidth Allocation Protocol (BACP) negotiation when no response to the drop requests arrives.
	<b>request</b>	Local router can initiate removal of a link. Enabled by default.
	<b>timer</b> <i>seconds</i>	Number of seconds to wait between drop requests sent.

## ppp bap link types

To specify the types of links that can be included in a specific multilink bundle, use the **ppp bap link types** interface configuration command. To remove a type of interface that was previously allowed to be added, use the **no** form of this command.

```
ppp bap link types [isdn] [analog]
```

```
no ppp bap link types [isdn] [analog]
```

Syntax Description		
	<b>isdn</b>	(Optional) ISDN interfaces can be added to a multilink bundle. This is the default.
	<b>analog</b>	(Optional) Asynchronous serial interfaces can be added to a multilink bundle.

## ppp bap max

To set upper limits on the number of retransmissions for PPP Bandwidth Allocation Protocol (BACP), use the **ppp bap max** interface configuration command. To remove any retry limit, use the **no** form of this command.

```
ppp bap max {dial-attempts number | ind-retries number | req-retries number | dialers number}
```

```
no ppp bap max {dial-attempts | ind-retries | req-retries | dialers number}
```

Syntax Description	
<b>dial-attempts</b> <i>number</i>	Maximum number of dial attempts to any destination number, in the range 1 to 3. The default is 1 dial attempt.
<b>ind-retries</b> <i>number</i>	Maximum number of retries of a call status indication message, in the range 1 to 10. The default is 3 indication retries.
<b>req-retries</b> <i>number</i>	Maximum number of retries for a particular request, in the range 1 to 5. The default is 3 request retries.
<b>dialers</b> <i>number</i>	Maximum number of free dialers logged, in the range 1 to 10. The default is 5 dialers.

## ppp bap monitor load

To validate peer requests to add or remove links against the current bundle load and the defined dialer load threshold, use the **ppp bap monitor load** interface configuration command. To specify that incoming link addition requests are not to be subject to the bundle load threshold, use the **no** form of this command.

**ppp bap monitor load**

**no ppp bap monitor load**

**Syntax Description** This command has no arguments or keywords.

## ppp bap number

To specify a local telephone number that peers can dial to establish a multilink bundle, use the **ppp bap number** interface configuration command. To remove a previously configured number, use the **no** form of this command.

**ppp bap number** { **default** *phone-number* | **secondary** *phone-number* | **prefix** *prefix-number* | **format national** | **format subscriber** }

**no ppp bap number** { **default** *phone-number* | **prefix** *prefix-number* | **format national** | **format subscriber** }

Syntax Description	
<b>default</b> <i>phone-number</i>	Primary (base) phone number for the interface and the number that can be used for incoming dial calls.
<b>secondary</b> <i>phone-number</i>	Telephone number for the second B channel. Applies only to BRI interfaces that have a different number for each B channel or to dialer interfaces that are BRIs.
<b>prefix</b> <i>prefix-number</i>	Prefix number for the PPP BAP phone number.
<b>format national</b>   <b>format subscriber</b>	Format for the primary phone number to be dialed should be either national or subscriber where the number of digits assigned to the number is as follows: <ul style="list-style-type: none"> <li>10-digit number for a national format.</li> <li>7-digit number for a subscriber format.</li> </ul>

## ppp bap timeout

To specify nondefault timeout values for PPP Bandwidth Allocation Protocol (BACP) pending actions and responses, use the **ppp bap timeout** interface configuration command. To reset the response timeout to the default value, or to remove a pending timeout entirely, use the **no** form of this command.

```
ppp bap timeout { pending seconds | response seconds }
```

```
no ppp bap timeout { pending | response }
```

<b>Syntax Description</b>	<b>pending</b> <i>seconds</i>	Number of seconds to wait before timing out pending actions, in the range 2 to 180 seconds. The default is 20 seconds.
	<b>response</b> <i>seconds</i>	Number of seconds to wait for a response before timing out, in the range 2 to 120 seconds. The default is 3 seconds.

## ppp bridge appletalk

To enable half-bridging of AppleTalk packets across a serial interface, use the **ppp bridge appletalk** interface configuration command. To disable AppleTalk packet half-bridging, use the **no** form of this command.

```
ppp bridge appletalk
```

```
no ppp bridge appletalk
```

**Syntax Description** This command has no arguments or keywords.

## ppp bridge ip

To enable half-bridging of IP packets across a serial interface, use the **ppp bridge ip** interface configuration command. To disable IP packet half-bridging, use the **no** form of this command.

```
ppp bridge ip
```

```
no ppp bridge ip
```

**Syntax Description** This command has no arguments or keywords.

## ppp bridge ipx

To enable half-bridging of Internetwork Packet Exchange (IPX) packets across a serial interface, use the **ppp bridge ipx** interface configuration command. To return to the default Novell Ethernet\_802.3 encapsulation, use the **no** form of this command.

```
ppp bridge ipx [novell-ether | arpa | sap | snap]
```

```
no ppp bridge ipx
```

### Syntax Description

<b>novell-ether</b>	(Optional) Novell Ethernet_802.3 encapsulation. This is the default.
<b>arpa</b>	(Optional) Novell Ethernet_II encapsulation.
<b>sap</b>	(Optional) Novell Ethernet_802.2 encapsulation.
<b>snap</b>	(Optional) Novell Ethernet_Snap encapsulation.

## ppp callback (DDR)

To enable a dialer interface to function either as a callback client that requests callback or as a callback server that accepts callback requests, use the **ppp callback** interface configuration command. To disable a function, use the **no** form of this command.

```
ppp callback {accept | permit | request}
```

```
no ppp callback
```

### Syntax Description

<b>accept</b>	Dialer interface accepts PPP callback requests (and functions as the PPP callback server).
<b>permit</b>	Dialer interface permits PPP callback (and functions as the PPP callback client).
<b>request</b>	Dialer interface requests PPP callback (and functions as the PPP callback client).

## ppp callback (PPP client)

To enable a PPP client to dial in to an asynchronous interface and request a callback, use the **ppp callback** interface configuration command. To disable callback acceptance, use the **no** form of this command.

```
ppp callback {accept | initiate}
```

```
no ppp callback
```

### Syntax Description

<b>accept</b>	Accept callback requests from RFC1570-compliant PPP clients on the interface.
<b>initiate</b>	Initiate a callback to non-RFC1570-compliant PPP clients dialing in to an asynchronous interface.

## ppp encrypt mppe

To enable Microsoft Point-to-Point Encryption (MPPE) on the virtual template, use the **ppp encrypt mppe** interface configuration command. To disable MPPE, use the **no** form of this command.

```
ppp encrypt mppe {auto | 40 | 128} [passive | required] [stateful]
```

```
no ppp encrypt mppe
```

### Syntax Description

<b>auto</b>	All available encryption strengths are allowed.
<b>40</b>	Only 40-bit encryption is allowed.
<b>128</b>	Only 128-bit encryption is allowed.
<b>passive</b>	(Optional) MPPE will not offer encryption, but will negotiate if the other tunnel endpoint requests encryption.
<b>required</b>	(Optional) MPPE must be negotiated, or the connection will be terminated.
<b>stateful</b>	(Optional) MPPE will only negotiate stateful encryption. If the <b>stateful</b> keyword is not used, MPPE will first attempt to negotiate stateless encryption, but will fall back to stateful if the other tunnel endpoint requests stateful.

## ppp ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer and so on, use the **ppp ipcp** command in template or interface configuration mode. To disable a **ppp ipcp** feature, use the **no** form of this command.

```
ppp ipcp {accept-address} | {dns {reject | accept | primary-ip-address [secondary-ip-address]
[accept]} | {ignore-map} | {username unique} | {wins {reject | accept | primary-ip-address
[secondary-ip-address] [accept]}}
```

```
no ppp ipcp {accept-address} | {dns [{reject | accept | primary-ip-address [secondary-ip-address]
[accept]}] | {ignore-map} | {username unique} | {wins [{reject | accept | primary-ip-address
[secondary-ip-address] [accept]}]}
```

### Syntax Description

<b>accept-address</b>	Accepts any non-zero IP address from the peer.
<b>dns</b>	Domain Name Server.
<b>reject</b>	Rejects the IPCP option if received from the peer.
<b>accept</b>	(Optional) Accepts a peer request for any non-zero server address.
<i>primary-ip-address</i>	(Optional) IP address of the primary DNS or WINS server.
<i>secondary-ip-address</i>	(Optional) IP address of the secondary DNS or WINS server.
<b>ignore-map</b>	Ignores dialer map when negotiating peer IP address.
<b>username unique</b>	Ignores a common username when providing an IP address to the peer.
<b>wins</b>	Windows Internet Naming Service.

## ppp lcp delay

To set a delay before initiating link control protocol (LCP) negotiations after a link connects, use the **ppp lcp delay** interface configuration command. To remove the delay, use the **no** form of this command.

**ppp lcp delay** *seconds*

**no ppp lcp delay** *seconds*

---

**Syntax Description**

<b>delay</b> <i>seconds</i>	Delay, in seconds, before initiating LCP negotiations.
-----------------------------	--

---

## ppp lcp fast-start

To allow a Point-to-Point (PPP) interface to respond immediately to incoming packets once a connection is established, use the **ppp lcp fast-start** interface configuration command. To specify that PPP delay before responding, use the **no** form of this command.

**ppp lcp fast-start**

**no ppp lcp fast-start**

---

**Syntax Description**

This command has no arguments or keywords.

## ppp link reorders

To set an advisory flag that indicates the serial interface may receive packets in a different order than a peer system sent them, use the **ppp link reorders** interface configuration command. To turn this flag off, use the **no** form of this command.

**ppp link reorders**

**no ppp link reorders**

---

**Syntax Description**

This command has no arguments or keywords.

## ppp max-bad-auth

To configure a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries, use the **ppp max-bad-auth** interface configuration command. To reset to the default of immediate reset, use the **no** form of this command.

**ppp max-bad-auth** *number*

**no ppp max-bad-auth**

---

### Syntax Description

<i>number</i>	Number of retries after which the interface is to reset itself. Default is 0.
---------------	---

---

## ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and Bandwidth Allocation Protocol (BAP) for dynamic bandwidth allocation, use the **ppp multilink** interface configuration command. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

**ppp multilink** [**bap**]

**no ppp multilink** [**bap** [**required**]]

---

### Syntax Description

<b>bap</b>	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
<b>required</b>	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

---

## ppp multilink fragment delay

To specify a maximum size in units of time for packet fragments on a Multilink PPP (MLP) bundle, use the **ppp multilink fragment delay** interface configuration command. To reset the maximum delay to the default value, use the **no** form of this command.

**ppp multilink fragment delay** *time*

**no ppp multilink fragment delay**

---

### Syntax Description

<i>time</i>	Maximum amount of time, in milliseconds, that it should take to transmit a fragment. The range is from 1 to 1000 milliseconds.
-------------	--

---

## ppp multilink fragment disable

To disable packet fragmentation, use the **ppp multilink fragment disable** interface configuration command. To enable fragmentation, use the **no** form of this command.

**ppp multilink fragment disable**

**no ppp multilink fragment disable**

---

**Syntax Description** This command has no arguments or keywords.

## ppp multilink fragment maximum

To set the maximum number of fragments a packet will be segmented into before being sent over the bundle, use the **ppp multilink fragment maximum** interface configuration command. To reset fragmentation to the default value, use the **no** form of this command.

**ppp multilink fragment maximum** *fragments*

**no ppp multilink fragment maximum**

---

**Syntax Description** *fragments* Maximum number of fragments in the range 1 to 16.

---

## ppp multilink group

To restrict a physical link to joining only a designated multilink-group interface, use the **ppp multilink group** interface configuration command. To remove the restrictions, use the **no** form of this command.

**ppp multilink group** *group-number*

**no ppp multilink group**

---

**Syntax Description** *group-number* Multilink-group number (a nonzero number).

---

## ppp multilink idle-link

To configure a multilink bundle so that the slowest link enters into receive-only mode when an additional link is added, use the **ppp multilink idle-link** interface configuration command. To remove the idle link flag, use the **no** form of this command.

```
ppp multilink idle-link
```

```
no ppp multilink idle-link
```

---

**Syntax Description** This command has no arguments or keywords.

## ppp multilink interleave

To enable interleaving of packets among the fragments of larger packets on a Multilink PPP (MLP) bundle, use the **ppp multilink interleave** interface configuration command. To disable interleaving, use the **no** form of this command.

```
ppp multilink interleave
```

```
no ppp multilink interleave
```

---

**Syntax Description** This command has no arguments or keywords.

## ppp multilink links maximum

To limit the maximum number of links that Multilink PPP (MLP) can dial for dynamic allocation, use the **ppp multilink links maximum** interface configuration command. To reset the default value, use the **no** form of this command.

```
ppp multilink links maximum links
```

```
no ppp multilink links maximum
```

---

**Syntax Description**

<i>links</i>	Maximum number of links, in the range 1 to 255.
--------------	---

---

## ppp multilink links minimum

To specify the preferred minimum number of links in a Multilink PPP (MLP) bundle, use the **ppp multilink links minimum** interface configuration command. To reset the default value, use the **no** form of this command.

**ppp multilink links minimum** *links*

**no ppp multilink links minimum**

### Syntax Description

<i>links</i>	Minimum number of links, in the range 0 to 255.
--------------	---

## ppp multilink load-threshold

To enable Multilink PPP (MLP) to monitor traffic load and prompt dialer capability to adjust bandwidth to fit the load, use the **ppp multilink load-threshold** interface configuration command. To disable this function, use the **no** form of this command.

**ppp multilink load-threshold** *load-threshold* [**outbound** | **inbound** | **either**]

**no ppp multilink load-threshold** *load-threshold* [**outbound** | **inbound** | **either**]

### Syntax Description

<i>load-threshold</i>	Load threshold at which to consider adding or dropping a link, expressed as a value in the range 1 to 255. A value of 255 indicates a 100 percent load. A value of 1 is a special case indicating any load at all; MLP will add as many links as it can, ignoring the actual traffic load.
<b>outbound</b>	(Optional) Only the outbound (transmit) traffic load is examined.
<b>inbound</b>	(Optional) Only the inbound (receive) traffic load is examined.
<b>either</b>	(Optional) Either the transmit or receive traffic load can trigger a link addition or subtraction.

## ppp quality

To enable Link Quality Monitoring (LQM) on a serial interface, use the **ppp quality** command in interface configuration mode. To disable LQM, use the **no** form of this command.

**ppp quality** *percentage*

**no ppp quality**

### Syntax Description

<i>percentage</i>	Specifies the link quality threshold. Range is 1 to 100.
-------------------	--

## ppp reliable-link

To enable Link Access Procedure, Balanced (LAPB) Numbered Mode negotiation for a reliable serial link, use the **ppp reliable-link** command in interface configuration mode. To disable negotiation for a PPP reliable link on a specified interface, use the **no** form of the command.

**ppp reliable-link**

**no ppp reliable-link**

---

**Syntax Description** This command has no arguments and keywords.

## ppp timeout authentication

To set PPP authentication timeout parameters, use the **ppp timeout authentication** interface configuration command. To reset the default value, use the **no** form of this command.

**ppp timeout authentication** *time*

**no ppp timeout authentication**

---

**Syntax Description**

<i>time</i>	Maximum time, in seconds, to wait for a response to an authentication packet.
-------------	---

---

## ppp timeout idle

To set PPP idle timeout parameters, use the **ppp timeout idle** interface configuration command. To reset the time value, use the **no** form of this command.

**ppp timeout idle** *time*

**no ppp timeout idle** *time*

---

**Syntax Description**

<i>time</i>	Line idle time, in seconds, allowed before disconnecting line.
-------------	--

---

## ppp timeout multilink link add

To limit the amount of time for which Multilink PPP (MLP) waits for a call to be established, use the **ppp timeout multilink link add** interface configuration command. To remove the value, use the **no** form of this command.

**ppp timeout multilink link add** *seconds*

**no ppp timeout multilink link add**

---

<b>Syntax Description</b>	<i>seconds</i>	Amount of time, in the range 1 to 65,535 seconds.
---------------------------	----------------	---

---

## ppp timeout multilink link remove

To set a timer that determines how long Multilink PPP (MLP) waits to drop a link when traffic load goes below the configured load threshold, use the **ppp timeout multilink link remove** interface configuration command. To remove the value, use the **no** form of this command.

**ppp timeout multilink link remove** *seconds*

**no ppp timeout multilink link remove**

---

<b>Syntax Description</b>	<i>seconds</i>	Amount of time, in the range 1 to 65,535 seconds.
---------------------------	----------------	---

---

## ppp timeout multilink lost-fragment

To set a timer that determines how long Multilink PPP (MLP) waits for an expected fragment to arrive before declaring it lost, use the **ppp timeout multilink lost-fragment** interface configuration command. To reset the value, use the **no** form of this command.

**ppp timeout multilink lost-fragment** *seconds*

**no ppp timeout multilink lost-fragment**

---

<b>Syntax Description</b>	<i>seconds</i>	Amount of time in the range 1 to 255 seconds.
---------------------------	----------------	---

---

## ppp timeout ncp

To set a time limit for the successful negotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp** interface configuration command. To reset the default condition, use the **no** form of this command.

**ppp timeout ncp** *time*

**no ppp timeout ncp**

<b>Syntax Description</b>	<i>time</i>	Maximum time, in seconds, PPP should for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected.
---------------------------	-------------	---

## ppp timeout retry

To set PPP timeout retry parameters, use the **ppp timeout retry** interface configuration command. To reset the time value, use the **no** form of this command.

**ppp timeout retry** *time*

**no ppp timeout retry**

<b>Syntax Description</b>	<i>time</i>	Maximum time, in seconds, to wait for a response during PPP negotiation.
---------------------------	-------------	--

## pptp flow-control receive-window

To specify how many packets the client can send before it has to wait for the tunnel server's acknowledgment, use the **pptp flow-control receive-window** VPDN configuration command. To return to the default value, use the **no** form of this command.

**pptp flow-control receive-window** *packets*

**no pptp flow-control receive-window**

<b>Syntax Description</b>	<i>packets</i>	Number of packets the client can send before it has to wait for the tunnel server's acknowledgment. The range is 1 to 64 packets.
---------------------------	----------------	---

## pptp flow-control static-rtt

To specify the timeout interval of the tunnel server between sending a packet to the client and receiving a response, use the **pptp flow-control static-rtt** VPDN configuration command. To return to the default value of 1500 milliseconds (ms), use the **no** form of this command.

**pptp flow-control static-rtt** *milliseconds*

**no pptp flow-control static-rtt**

<b>Syntax Description</b>	<i>milliseconds</i>	Timeout interval of the tunnel server between sending a packet to the client and receiving a response. The range is 100 to 5000 milliseconds.
---------------------------	---------------------	---

## pptp tunnel echo

To specify the period of idle time on the tunnel that will trigger an echo message from the tunnel server to the client, use the **pptp tunnel echo** VPDN configuration command. To return to the default value of 60 seconds, use the **no** form of this command.

**pptp tunnel echo** *seconds*

**no pptp tunnel echo**

<b>Syntax Description</b>	<i>seconds</i>	Echo packet interval in seconds. The range is 0 to 1000 seconds.
---------------------------	----------------	--

## pri-group timeslots nfas\_d

To configure Non-Facility Associated Signalling (NFAS) and specify the channels to be controlled by the primary NFAS D channel, use the **pri-group timeslots nfas\_d** controller configuration command.

**pri-group timeslots** *range nfas\_d* [**primary** | **backup** | **none**] *nfas\_interface number nfas\_group number*

**pri-group timeslots** *range*

<b>Syntax Description</b>	<i>range</i>	Channels in the range 1 to 24. A range of channels is shown with a hyphen (-).
	<b>primary</b>	(Optional) Function of channel 24: the primary NFAS D channel.
	<b>backup</b>	(Optional) Function of channel 24: the backup NFAS D channel.
	<b>none</b>	(Optional) Function of channel 24: B channel.
	<b>nfas_interface number</b>	Value assigned by the service provider to ensure unique identification of a PRI interface.
	<b>nfas_group number</b>	Group identifier unique on the router. Multiple NFAS groups can exist on the router.

## profile incoming

To define a template formed by directives guiding the Call Service Module (CSM) to process the digit sequence for a signaling class, use the **profile incoming** global configuration command.

**profile incoming** *template*

---

### Syntax Description

*template*

String of special characters that are arranged in a certain order to process the digit sequence for the signaling class. Choose from the following list:

- **S**—Starts the state machine.
  - **<\***—Waits for the digit **\*** to be detected. The digit to be detected is the next character in the template. If any other digit is detected, then that is a failure. If the digit is detected, then go to the next directive.
  - **a**—Digits are collected as the ANI until the first nondigit or a timeout occurs.
  - **d**—Digits are collected as the DNIS until the first nondigit or a timeout occurs.
  - **n**—Notifies the CSM of the collected ANI and DNIS.
- 

## protocol rlm port

To configure the RLM port number, use the **protocol rlm port** RLM configuration command. To disable this function, use the **no** form of this command.

**protocol rlm port** *port-number*

**no protocol rlm port** *port-number*

---

### Syntax Description

*port-number*

RLM port number. See Table 45 for the port number choices.

---

**Table 45** Default RLM Port Number

Protocol	Port Number
RLM	3000
ISDN	Port[RLM]+1

## protocol (VPDN)

To specify the Layer 2 Tunneling Protocol (L2TP) that the virtual private dialup network (VPDN) subgroup will use, use the **protocol** VPDN subgroup command. To remove the protocol-specific configurations from a VPDN subgroup, use the **no** form of this command.

```
protocol {l2f | l2tp | pppoe | any}
```

```
no protocol
```

### Syntax Description

<b>l2f</b>	Layer 2 Forwarding (L2F) tunnels.
<b>l2tp</b>	Layer 2 Transport Protocol (L2TP) tunnels.
<b>pppoe</b>	Enables the VPDN subgroup to establish PPPoE sessions.
<b>any</b>	Either L2F or L2TP tunnels.

## range

To associate a range of modems or other physical resources with a resource group, use the **range** resource group configuration command. To remove a range of modems or other physical resources, use the **no** form of this command.

```
range {limit number | port range}
```

```
no range {limit number | port range}
```

### Cisco AS5200 and AS5300 Series Routers

```
range {limit number | port slot/port slot/port}
```

```
no range {limit number | port slot/port slot/port}
```

### Syntax Description

<b>limit number</b>	Maximum number of simultaneous connections supported by the resource group. Replace the <i>number</i> argument with the session limit you want to assign. Your access server hardware configuration determines the maximum value of this limit. Applicable to ISDN B-channels or HDLC controllers.
<b>port range</b>	Range of resource ports to use in the resource group.
<b>port slot/port</b>	Specific ports to use in the resource group.

## rcapi number

To enable the Cisco 800 series router to distinguish between incoming CAPI calls and incoming non-CAPI calls such as POTS, PPP, and X.25, use the **rcapi number** global configuration command. To release the specified directory number from the RAPI interface, use the **no** form of this command.

**rcapi number** *directory-number*[:*subaddress*]

**no rcapi number**

### Syntax Description

<i>directory-number</i>	ISDN directory number. Default is <i>none</i> .
<i>:subaddress</i>	(Optional) Subaddress of the router preceded by a colon (:).

## rcapi server

To enable the RAPI server on the 800 series router or to set the TCP port number, use the **rcapi server** global configuration command. To disable the RAPI server on the 800 series router, use the **no** form of this command.

**rcapi server** [*port number*]

**no rcapi server**

### Syntax Description

<i>port number</i>	(Optional) TCP port number. Default is 2578.
--------------------	--

## reload

To reload a configuration on a Cisco access server, use the **reload** privileged EXEC command. To cancel the reload, use the **reload cancel** command.

**reload** [*description-line* | **at** *hh:mm* | **in** [*hhh:*]*mmm*]

**reload cancel**

### Syntax Description

<i>description-line</i>	Displays reason for the reload, 1 to 255 characters in length.
<b>at</b> <i>hh:mm</i>	Schedules when the software reload takes place using a 24-hour clock. If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.
<b>in</b> [ <i>hhh:</i> ] <i>mmm</i>	Schedule a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
<b>cancel</b>	Cancels a scheduled reload.

## reload components

To request that the DSC (or DSCs in a redundant configuration) be reloaded at the same time as a reload on the Router Shelf on the Cisco AS5800, use the **reload components EXEC** command. To cancel a reload, use the **reload components cancel** command.

```
reload components { all | description-line | at hh:mm | in [hhh:]mmm }
```

```
reload components cancel
```

Syntax Description		
<b>all</b>		Reloads all attached components.
<i>description-line</i>		Displays reason for the reload, 1 to 255 characters in length.
<b>at</b> <i>hh:mm</i>		Schedules when the software reload takes place using a 24-hour clock. If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.
<b>in</b> [ <i>hhh:</i> ] <i>mmm</i>		Schedule a reload of the software to take effect in the specified minutes or (optionally) hours and minutes. The reload must take place within approximately 24 days.
<b>cancel</b>		Cancels a scheduled reload.

## request dialin

To configure a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, use the **request dialin VPDN group** command. To remove the request-dialin subgroup from a VPDN group, use the **no** form of this command.

```
request dialin
```

```
no request dialin
```

Syntax Description	
	This command has no arguments or keywords.

## request dialout

To enable an L2TP network server (LNS) to request virtual private dialup network (VPDN) dial-out calls by using Layer 2 Tunnel Protocol (L2TP), use the **request dialout** VPDN group configuration command. To disable L2TP dialout, use the **no** form of this command.

**request dialout**

**no request dialout**

### Syntax Description

This command has no arguments or keywords.

## resource

To assign resources and supported call-types to a customer profile, use the **resource** customer profile configuration command. To disable this function, use the **no** form of this command.

**resource** *name* { **digital** | **speech** | **v110** | **v120** } [**service** *name*]

**no resource** *name* { **digital** | **speech** | **v110** | **v120** } [**service** *name*]

### Syntax Description

<i>name</i>	Name for a group of physical resources inside the access server. This name can have up to 23 characters.
<b>digital</b>	Accepts digital calls. Specifies circuit-switched data calls that terminate on a HDLC framers (unlike asynchronous analog modem call that use start and stop bits).
<b>speech</b>	Accepts speech calls. Specifies normal voice calls, such as calls started by analog modems and standard telephones.
<b>v110</b>	Accepts V.110 calls.
<b>v120</b>	Accepts V.120 calls. By specifying this keyword, the access server begins counting the number of v120 software encapsulations occurring in the system.
<b>service</b> <i>name</i>	(Optional) Name for a service profile. This option is not supported for digital or V.120 calls.

## resource-pool

To enable or disable resource pool management, use the **resource-pool** global configuration command.

**resource-pool** { **enable** | **disable** }

### Syntax Description

<b>enable</b>	Enables resource pool management.
<b>disable</b>	Disables resource pool management.

## resource-pool aaa accounting ppp

To include enhanced start/stop resource manager records to authorization, authentication, and accounting (AAA) accounting, use the **resource-pool aaa accounting ppp** global configuration command. To disable this feature, use the **no** form of this command.

**resource-pool aaa accounting ppp**

**no resource-pool aaa accounting ppp**

**Syntax Description** This command has no arguments or keywords.

## resource-pool aaa protocol

To specify which protocol to use for resource management, use the **resource-pool aaa protocol** global configuration command. To disable this feature and go to local, use the **no** form of this command.

**resource-pool aaa protocol {local | group *name*}**

**no resource-pool aaa protocol**

<b>Syntax Description</b>	<b>local</b>	Local authorization.
	<b>group <i>name</i></b>	Use an external authorization, authentication, and accounting (AAA) server group. The Resource Pool Management Server (RPMS) is defined in a AAA server group.

## resource-pool call treatment

To set up the signal sent back to the telco switch in response to incoming calls, use the **resource-pool call treatment** global configuration command. To disable this function, use the **no** form of this command.

**resource-pool call treatment {profile {busy | no-answer} | resource {busy | channel-not-available}}**

**no resource-pool call treatment {profile {busy | no-answer} | resource {busy | channel-not-available}}**

<b>Syntax Description</b>	<b>profile</b>	Call treatment when profile authorization fails.
	<b>busy</b>	Answers the call, then sends a busy signal when profile authorization or resource allocation fails.
	<b>no-answer</b>	Does not answer the call when profile authorization fails.
	<b>resource</b>	Call treatment when resource allocation fails.
	<b>channel-not-available</b>	Sends channel not available (CNA) code when resource allocation fails.

## resource-pool call treatment discriminator

To modify the signal (ISDN cause code) sent to the switch when a discriminator rejects a call, enter the **resource-pool call treatment discriminator** global configuration command. To disable this function, use the **no** form of this command.

**resource-pool call treatment discriminator** { **busy** | **no-answer** | **channel-not-available** }

**no resource-pool call treatment discriminator** { **busy** | **no-answer** | **channel-not-available** }

### Syntax Description

<b>busy</b>	Answers the call, then sends a busy signal when profile authorization or resource allocation fails.
<b>no-answer</b>	Does not answer the call when profile authorization fails.
<b>channel-not-available</b>	Sends channel not available (CNA) code when resource allocation fails.

## resource-pool group resource

To create a resource group for resource management, use the **resource-pool group resource** global configuration command. To remove a resource group from the running configuration, use the **no** form of this command.

**resource-pool group resource** *name*

**no resource-pool group resource** *name*

### Syntax Description

<i>name</i>	Name for the group of physical resources inside the access server. This name can have up to 23 characters.
-------------	--

## resource-pool profile customer

To create a customer profile, use the **resource-pool profile customer** global configuration command. To delete a customer profile from the running configuration, use the **no** form of this command.

**resource-pool profile customer** *name*

**no resource-pool profile customer** *name*

### Syntax Description

<i>name</i>	Customer profile name. This name can have up to 23 characters.
-------------	--

## resource-pool profile discriminator

To create a call discrimination profile and assign it a name, use the **resource-pool profile discriminator** global configuration command. To remove a call discrimination profile from the running configuration, use the **no** form of this command.

**resource-pool profile discriminator** *name*

**no resource-pool profile discriminator** *name*

---

### Syntax Description

<i>name</i>	Name of the call discrimination profile created. This name can have up to 23 characters. You can add a CLID or DNIS group to the discriminator profile created.
-------------	---

---

## resource-pool profile service

To set up the service profile configuration, use the **resource-pool profile service** global configuration command. To disable this function, use the **no** form of this command.

**resource-pool profile service** *name*

**no resource-pool profile service** *name*

---

### Syntax Description

<i>name</i>	Service profile name. This name can have up to 23 characters.
-------------	---

---

## resource-pool profile vpdn

To set up for virtual private dialup network (VPDN) session counting for one or more VPDN groups and to limit sessions that can be authorized for VPDN groups, use the **resource-pool profile vpdn** global configuration command. To disable this function, use the **no** form of this command.

**resource-pool profile vpdn** *name*

**no resource-pool profile vpdn** *name*

---

### Syntax Description

<i>name</i>	VPDN profile name.
-------------	--------------------

---

## retry keepalive

To enable Redundant Link Manager (RLM) keepalive retries, use the **retry keepalive** RLM configuration command. To disable this function, use the **no** form of this command.

**retry keepalive** *number-of-times*

**no retry keepalive** *number-of-times*

<b>Syntax Description</b>	<i>number-of-times</i>	Number of keepalive failures allowed before the link is declared down, from 1 to 100.
---------------------------	------------------------	---

## rotary

To define a group of lines consisting of one or more virtual terminal lines or one auxiliary port line, use the **rotary** line configuration command. To remove a group of lines from a rotary group, use the **no** form of this command.

**rotary** *group* [**queued**]

**no rotary**

<b>Syntax Description</b>	<i>group</i>	Rotary group number.
	<b>queued</b>	(Optional) Queues a connection request to a rotary group.

## rotary-group

To assign a request-dialout virtual private dialup network (VPDN) subgroup to a dialer rotary group, use the **rotary-group** request-dialout configuration command. To remove the request-dialout VPDN subgroup from the dialer rotary group, use the **no** form of this command.

**rotary-group** *group-number*

**no rotary-group** [*group-number*]

<b>Syntax Description</b>	<i>group-number</i>	The dialer rotary group that this VPDN group belongs to.
---------------------------	---------------------	--

## script activation

To specify that a chat script start on a physical terminal line any time the line is activated, use the **script activation** line configuration command. To disable this feature, use the **no** form of this command.

**script activation** *regular-expression*

**no script activation**

---

### Syntax Description

*regular-expression* Regular expression that specifies the set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument will be used.

---

## script arap-callback

To specify that a chat script start on a line any time an AppleTalk Remote Access (ARA) client requests a callback, use the **script arap-callback** line configuration command. To disable this feature, use the **no** form of this command.

**script arap-callback** *regular-expression*

**no script arap-callback**

---

### Syntax Description

*regular-expression* Regular expression that specifies the set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument is used.

---

## script callback

To specify that a chat script start on a line any time a client requests a callback, use the **script callback** line configuration command. To disable this feature, use the **no** form of this command.

**script callback** *regular-expression*

**no script callback**

---

### Syntax Description

*regular-expression* Regular expression that specifies the set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument is used.

---

## script connection

To specify that a chat script will start on a physical terminal line any time a remote network connection is made to a line, use the **script connection** line configuration command. To disable this feature, use the **no** form of this command.

**script connection** *regular-expression*

**no script connection**

---

**Syntax Description**

*regular-expression* Set of modem scripts that can be executed. The first script name that matches the *regular-expression* argument will be used.

---

## script dialer

To specify a default modem chat script, use the **script dialer** line configuration command. To disable this feature, use the **no** form of this command.

**script dialer** *regular-expression*

**no script dialer**

---

**Syntax Description**

*regular-expression* Set of modem scripts that can be executed. The first script that matches the *regular-expression* argument will be used.

---

## script reset

To specify that a chat script will start on a physical terminal line any time the specified line is reset, use the **script reset** line configuration command. To disable this feature, use the **no** form of this command.

**script reset** *regular-expression*

**no script reset**

---

**Syntax Description**

*regular-expression* Set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument will be used.

---

## script startup

To specify that a chat script will start on a physical terminal line any time the router is powered up, use the **script startup** line configuration command. To disable this feature, use the **no** form of this command.

**script startup** *regular-expression*

**no script startup**

---

<b>Syntax Description</b>	<i>regular-expression</i> Set of modem scripts that might be executed. The first script that matches the <i>regular-expression</i> argument will be used.
---------------------------	---

---

## server (RLM)

To identify an RLM server, use the **server** RLM configuration command. To remove the identification, use the **no** form of this command

**server** *name-tag*

**no server** *name-tag*

---

<b>Syntax Description</b>	<i>name-tag</i> Name to identify the server configuration so that multiple entries of server configuration can be entered.
---------------------------	--

---

## sgbp dial-bids

To allow the stack group to bid for dialout connection, use the **sgbp dial-bids** global configuration command. To disable this function, use the **no** form of this command.

**sgbp dial-bids**

**no sgbp dial-bids**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## sgbp group

To define a named stack group and make this router a member of that stack group, use the **sgbp group** global configuration command. To remove the definition, use the **no** form of this command.

**sgbp group** *name*

**no sgbp group**

---

### Syntax Description

<i>name</i>	Name of the stack group the system belongs to.
-------------	--

---

## sgbp member

To specify the host name and IP address of a router or access server that is a peer member of a stack group, use the **sgbp member** global configuration command. To remove the member association, use the **no** form of this command.

**sgbp member** *peer-name* [*peer-ip-address*]

**no sgbp member** *peer-name*

---

### Syntax Description

<i>peer-name</i>	Host name of the peer member.
<i>peer-ip-address</i>	(Optional) IP address of the peer member. If the domain name system (DNS) can perform a lookup on the <i>peer-name</i> value, the IP address is not required. Otherwise, it must be specified.

---

## sgbp ppp-forward

To enable forwarding of PPP calls—in addition to Multilink PPP (MLP) calls—to the winner of the Stack Group Bidding Protocol (SGBP) bid, use the **sgbp ppp-forward** global configuration command. To return to the default state, use the **no** form of this command.

**sgbp ppp-forward**

**no sgbp ppp-forward**

---

### Syntax Description

This command has no arguments or keywords.

## sgbp seed-bid

To set the bidding level that a stack group member can bid with for a bundle, use the **sgbp seed-bid** global configuration command. To return to the default state, use the **no** form of this command.

```
sgbp seed-bid {default | offload | forward-only | bid}
```

```
no sgbp ppp-forward
```

Syntax Description		
<b>default</b>		If set across all members of a stack group, indicates that the member which receives the first call for a certain user always wins the bid and hosts the master bundle interface. All subsequent calls to the same user received by another stack group member will <i>project</i> to this stackgroup member. This is the default.
<b>offload</b>		Indicates that this router is a relatively higher powered stack group member, is to function as an offload server, and host the master bundle interface.
<b>forward-only</b>		Indicates that this router or access server is to forward calls to another system and never wins the bid to host a master interface. This router or access server should hang up—instead of answering a call—if all the offload servers are down.
	<i>bid</i>	Bid level, an integer in the range 0 through 9999.

## shelf-id

To change the shelf number assigned to the router shelf or dial shelf on the Cisco AS5800, use the **shelf-id** global configuration command. To return the shelf numbers to the default value, use the **no** form of this command.

```
shelf-id number {router-shelf | dial-shelf}
```

```
no shelf-id number
```

Syntax Description		
	<i>number</i>	Number to assign to the shelf. Range: 0 to 9999.
	<b>router-shelf</b>	Specified number to the router shelf.
	<b>dial-shelf</b>	Specified number to the dial shelf.



## Dial Technologies Commands: **show async status** Through **show rlm group timer**

---

This chapter describes the function and syntax of the dial technologies commands: **show async status** through **show rlm group timer**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Dial Technologies Command Reference*.

### **show async status**

To display the status of activity on all lines configured for asynchronous support, use the **show async status** privileged EXEC command.

```
show async status
```

---

**Syntax Description** This command has no arguments or keywords.

### **show busyout**

To display the busyout status for a card on the dial shelf, use the **show busyout** privileged EXEC command.

```
show busyout shelfslot/port
```

---

**Syntax Description** *shelfslot/port* Shelf, slot, and port number; for example, 1/0/5. The forward slash (/) is required.

---

## show call calltracker active

To display all information stored within the Call Tracker active database for all active calls, use the **show call calltracker active** privileged EXEC command.

```
show call calltracker active [category [isdn | modem | other | v110 | v120]]
```

---

### Syntax Description

<b>category</b>	(Optional) Displays Call Tracker data for a specific type of call. The default is to show all calls, regardless of type. By specifying the <b>category</b> keyword with one of the optional modem type keywords, Call Tracker only shows calls whose records indicate that category.
-----------------	--

---

## show call calltracker handle

To display all information stored within the Call Tracker active or history database table for a specified unique call handle identifier, use the **show call calltracker handle** privileged EXEC command.

```
show call calltracker handle handle
```

---

### Syntax Description

<i>handle</i>	Unique call identifier assigned by Call Tracker from the moment a DS0 B channel is requested. This identifier is a sequential number starting with handle 1.
---------------	--

---

## show call calltracker history

To display all information stored within the Call Tracker history database table for the most recent disconnected calls, use the **show call calltracker history** privileged EXEC command.

```
show call calltracker history [category [isdn | modem | other | v110 | v120]]
```

---

### Syntax Description

<b>category</b>	(Optional) Displays Call Tracker history data for a specific type of call. The default is to show all calls, regardless of type. By specifying the <b>category</b> keyword with one of the optional modem type keywords, Call Tracker will only show calls whose records indicate that category.
-----------------	--

---

## show call calltracker summary

To display Call Tracker activity and configuration information such as the number of active calls and the history table attributes, use the **show call calltracker summary** privileged EXEC command.

```
show call calltracker summary
```

---

### Syntax Description

This command has no arguments or keywords.

## show call progress tone

To display the contents of the internal call progress (CP) tone database for a specific country, use the **show call progress tone** EXEC command.

```
show call progress tone country [tone-type]
```

Syntax Description	
<i>country</i>	Enters the country code for the country's call progress tone database you want to see.
<i>tone-type</i>	(Optional) Enters the tone type parameters you want to see from Table 46.

**Table 46 Supported Tone Type Parameters**

<b>busy</b>	—Busy tone
<b>congestion</b>	—Congestion tone
<b>dialtone</b>	—Dial tone
<b>disconnect</b>	—Disconnect tone
<b>error</b>	—Error tone
<b>off-hook-alert</b>	—Off-hook alert tone
<b>off-hook-notice</b>	—Off-hook notice tone
<b>pbx-dialtone</b>	—PBX dialtone
<b>ringback</b>	—Ringback tone
<b>routing</b>	—Routing tone

## show caller

To display caller information, enter the **show caller** EXEC command.

```
show caller [{full | {interface {Async | Dialer | Serial}} | line {range | line-modem-options} |  
summary | timeouts | user name [detailed]]]
```

Syntax Description	
<b>full</b>	(Optional) Provides expanded caller information.
<b>interface</b>	(Optional) Displays a summary of caller information for the interface name you provide:  <b>Async</b> —Async interface number in the range 1 to 169. <b>Dialer</b> —Dialer interface number in the range 0 to 799. <b>Serial</b> —Serial interface number in the range 0 to 3.

<b>line range l</b> <i>line-modem-options</i>	(Optional) Displays a summary of caller information for the lines you specify, in the range 0 to 54, or by line or modem options, as follows: <b>aux</b> —Auxiliary line. <b>console</b> —Primary terminal line. <b>tty</b> —Terminal controller. <b>v110</b> —V.110 modem standard information. <b>vtty</b> —Virtual terminal line. <i>x/y</i> —Internal modem slot/port.
<b>summary</b>	(Optional) Displays total users logged and total ISDN/Analog users since the last <b>reload</b> command was entered.
<b>timeouts</b>	(Optional) Displays session and idle limits and disconnect time.
<b>user name</b>	Displays a summary of caller information for the username you provide.
<b>detailed</b>	Provides expanded information about the username specified.

## show controllers bri

To display information about the ISDN BRI, use the **show controllers bri** privileged EXEC command.

### Cisco MC3810 Routers

```
show controllers bri [number]
```

### Cisco 7200 Series Routers

```
show controllers bri slot/port
```

### All Other Routers

```
show controllers bri number
```

<b>Syntax Description</b>	<i>number</i>	Interface number. The value is 0 through 7 if the router has one 8-port BRI network interface module (NIM), or 0 through 15 if the router has two 8-port BRI NIMs. Interface number values will vary, depending on the hardware platform used. The Cisco 3600 series router for example, can have up to 48 interfaces. Valid BRI controller numbers for the Cisco MC3810 router are from 1 to 4.
	<i>slot/port</i>	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.

## show controllers e1

To display information about E1 links, use the **show controllers e1** privileged EXEC command.

### Cisco 4000 Series Routers

```
show controllers e1 controller-number
```

### Cisco 7500 Series Routers

```
show controllers e1 [slot/port]
```

### Cisco AS5000 Series Access Servers

```
show controllers e1 {controller-number | clock | firmware-status | monitor | timeslots range}
```

Syntax Description	
<i>controller-number</i>	Controller number. the controller number.
<i>slot/port</i>	(Optional) Backplane slot number and port number on the interface. See the hardware manuals for your controller type to determine specific slot and port numbers.
<b>clock</b>	Displays primary clock change history.
<b>firmware-status</b>	Displays system crash history.
<b>monitor</b>	Displays primary monitor change history.
<b>timeslots</b> <i>timeslot-range</i>	Displays DS0 information. Time slot range is 1 through 31 for the E1 controller.

## show controllers e1 call-counters

To view the total number of calls and call durations on an E1 controller, use the **show controllers e1 call-counters** privileged EXEC command.

```
show controllers e1 number call-counters
```

Syntax Description	
<i>number</i>	Controller number (for example, 0, 1, 2, or 3).

## show controllers e1 cas-data

To display internal call switching module information about the switched 56K data channels, use the **show controllers e1 cas-data** privileged EXEC command.

```
show controllers e1 number cas-data
```

Syntax Description	
<i>number</i>	Controller number (for example, 0, 1, 2, or 3).

## show controllers t1 call-counters

To view the total number of calls and call durations on a T1 controller, use the **show controllers t1 call-counters** privileged EXEC command.

```
show controllers t1 number call-counters
```

Syntax Description	<i>number</i>	Controller number (for example, 0, 1, 2, or 3).
--------------------	---------------	---

## show controllers t1 cas-data

To display internal call switching module information about the switched 56K data channels, use the **show controllers t1 cas-data** privileged EXEC command.

```
show controllers t1 number cas-data
```

Syntax Description	<i>number</i>	Controller number (for example, 0, 1, 2, or 3).
--------------------	---------------	---

## show controllers t1 timeslots

To show the CAS and ISDN PRI state in detail, use the **show controllers t1 timeslots** EXEC command.

```
show controllers t1 controller-number timeslots timeslot-range
```

### Cisco AS5000 Series Access Servers

```
show controllers t1 {controller-number | clock | firmware-status | timeslots timeslot-range}
```

Syntax Description	<i>controller-number</i>	Controller number.
	<b>timeslots</b> <i>timeslot-range</i>	Displays DS0 information. Time slot range is 1 through 31 for the E1 controller.
	<b>clock</b>	Displays primary clock change history.
	<b>firmware-status</b>	Displays system crash history.

## show cot dsp

To display information about the Continuity Test (COT) Digital Signal Processor configuration (DSP) or current status, use the **show cot dsp** privileged EXEC command.

### Cisco AS5200 and Cisco AS5300

```
show cot dsp {config | status} applique/ds0
```

### Cisco AS5800

```
show cot dsp {config | status} shelf/slot/applique/ds0
```

Syntax Description		
	<b>config</b>	Displays the COT DSP configuration.
	<b>status</b>	Displays the COT DSP status.
	<i>applique</i>	ID of the hardware unit that provides the external interface connections from a router to the network. Number of COT operation request.
	<i>ds0</i>	Number of COT operation request.
	<i>shelf</i>	Shelf ID of COT operation request.
	<i>slot</i>	Designates the slot number, 0 to 2.
	<i> </i>	Separates each argument.

## show cot request

To display information about COT operation requests, use the **show cot request** privileged EXEC command.

### Cisco AS5200 and Cisco AS5300

```
show cot request shelf/slot/applique/ds0
```

### Cisco AS5800

```
show cot request applique/ds0
```

Syntax Description		
	<i>shelf</i>	Shelf ID of COT operation request.
	<i>slot</i>	Designate the slot number, 1 to 4.
	<i>applique</i>	Hardware unit that provides the external interface connections from a router to the network. Number of COT operation request.
	<i>ds0</i>	Number of COT operation request.
	<i> </i>	Separates each argument.

## show cot summary

To display information about the Continuity Test (COT) activity, use the **show cot summary** privileged EXEC command.

```
show cot summary
```

---

**Syntax Description** This command has no arguments or keywords.

## show dhcp

To display the current DHCP (Dynamic Host Configuration Protocol) settings on point-to-point interfaces, use the **show dhcp** privileged EXEC command.

```
show dhcp {server | lease [interface async [number]]}
```

---

<b>Syntax Description</b>	<b>server</b>	Displays known DHCP servers.
	<b>lease</b>	Displays DHCP addresses leased from a server.
	<b>interface async</b> <i>[number]</i>	(Optional) Specifies asynchronous interfaces and, optionally, a specific interface number.

---

## show dialer

To display general diagnostic information for interfaces configured for DDR (dial-on-demand routing), use the **show dialer** command in EXEC mode.

```
show dialer [interface type number]
```

---

<b>Syntax Description</b>	<b>interface</b>	(Optional) Displays information for the interface specified by the arguments <i>type</i> and <i>number</i> .
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

---

## show dialer dnis

To see how many calls DNIS groups have had, use the **show dialer dnis** privileged EXEC command.

```
show dialer dnis {group [name] | number [number]}
```

Syntax Description		
	<b>group</b>	Displays DNIS group statistics.
	<i>name</i>	(Optional) DNIS group name.
	<b>number</b>	Displays DNIS group number statistics.
	<i>number</i>	(Optional) DNIS group number.

## show dialer interface bri

To display general diagnostic information for ISDN BRI interfaces configured for DDR (dial-on-demand routing), use the **show dialer interface bri** command in EXEC mode.

```
show dialer interface bri number
```

Syntax Description		
	<i>number</i>	BRI interface number.

## show dialer map

To display configured dynamic and static dialer maps and dynamically created PPP BACP temporary static dialer maps, use the **show dialer map** command in EXEC mode.

```
show dialer map
```

Syntax Description	
	This command has no arguments or keywords.

## show dialer sessions

To display all dialer sessions, use the **show dialer sessions** command in EXEC configuration mode.

```
show dialer sessions
```

Syntax Description	
	This command has no arguments or keywords.

## show dial-shelf

To display information about the dial shelf, including clocking information, use the **show dial-shelf** user or privileged EXEC command.

```
show dial-shelf [clocks | slot slot-number [clocks]]
```

Syntax Description		
	<b>clocks</b>	(Optional) Displays the current primary and backup clocks along with their priorities.
	<b>slot <i>slot-number</i></b>	(Optional) Displays information for a specific slot. <i>Slot-number</i> can be from 0 to 14.

## show dial-shelf split

To display information about the types of cards in nonowned dial shelf slots, use the **show dial-shelf split** user or privileged EXEC command.

```
show dial-shelf split
```

Syntax Description	
	This command has no arguments or keywords.

## show dsc clock

To display information about the dial shelf controller clock, use the **show dsc clock** privileged EXEC command with the line card execute (**execute-on**) command.

```
execute-on slot-number show dsc clock
```

Syntax Description		
	<i>slot-number</i>	Displays information for a specific slot. Slot number (12 or 13) must be occupied by a DSC card.

## show dsi

To display information about the dial shelf interconnect (DSI) port adapter parameters, use the **show dsi** privileged EXEC command with the line card execute (**execute-on**) command.

```
execute-on show dsi
```

Syntax Description	
	This command has no arguments or keywords.

## show dsip

To display all information about the Distributed System Interconnect Protocol (DSIP) on a Cisco AS5800, use the **show dsip** EXEC command.

```
show dsip
```

---

**Syntax Description** This command has no arguments or keywords.

## show dsip clients

To display information about Distributed System Interconnect Protocol (DSIP) clients, use the **show dsip clients** EXEC command.

```
show dsip clients
```

---

**Syntax Description** This command has no arguments or keywords.

## show dsip nodes

To display information about the processors running the Distributed System Interconnect Protocol (DSIP), use the **show dsip nodes** EXEC command.

```
show dsip nodes
```

---

**Syntax Description** This command has no arguments or keywords.

## show dsip ports

To display information about local and remote ports, use the **show dsip ports** EXEC command.

```
show dsip ports [local | remote [slot]]
```

---

<b>Syntax Description</b>	<b>local</b>	(Optional) Displays information for local ports. The local port is the port created at a seat's local end.
	<b>remote</b>	(Optional) Displays information for remote ports. The remote port is the port residing on a remote seat to which DSIP IPC based connection is open.
	<i>slot</i>	(Optional) Specifies a slot number to display information for a specific card on the dial shelf.

---

## show dsip queue

To display the number of IPC messages in the transmission queue waiting for acknowledgment, use the **show dsip queue** EXEC command.

```
show dsip queue
```

---

**Syntax Description** This command has no arguments or keywords.

## show dsip tracing

To display Distributed System Interconnect Protocol (DSIP) tracing buffer information, use the **show dsip tracing** EXEC command.

```
show dsip tracing [control | data | ipc] [slot | entries entry-number [slot]]
```

---

<b>Syntax Description</b>	<b>control</b>	(Optional) Displays the control tracing buffer.
	<b>data</b>	(Optional) Displays the data tracing buffer.
	<b>ipc</b>	(Optional) Displays the inter-process communication tracing buffer.
	<i>slot</i>	(Optional) Specifies a specific slot number on the dial shelf. Slot number can be 0 to 14.
	<b>entries entry-number</b>	(Optional) Specifies the number of entries to trace. Entries can be 1 to 500.

---

## show dsip transport

To display information about the Distributed System Interconnect Protocol (DSIP) transport statistics for the control/data and IPC packets and registered addresses, use the **show dsip transport** EXEC command.

```
show dsip transport
```

---

**Syntax Description** This command has no arguments or keywords.

## show dsip version

To display Distributed System Interconnect Protocol (DSIP) version information, use the **show dsip version** EXEC command.

```
show dsip version
```

---

**Syntax Description** This command has no arguments or keywords.

## show interfaces bri

To display information about the BRI D channel or about one or more B channels, use the **show interfaces bri** privileged EXEC command.

```
show interfaces bri number[:bchannel] | [first] [last] [accounting]
```

### Cisco 7200 Series Router only

```
show interfaces bri slot/port
```

Syntax Description	
<i>number</i>	Interface number. The value is 0 through 7 if the router has one 8-port BRI NIM or 0 through 15 if the router has two 8-port BRI NIMs. Interface number values will vary, depending on the hardware platform used. The Cisco 3600 series router, for example, can have up to 48 interfaces.  Specifying just the number will display the D channel for that BRI interface.
<i>slot/port</i>	On the Cisco 7200 series, slot location and port number of the interface.
<i>:bchannel</i>	(Optional) Colon (:) followed by a specific B channel number.
<i>first</i>	(Optional) Specifies the first of the B channels; the value can be either 1 or 2.
<i>last</i>	(Optional) Specifies the last of the B channels; the value can only be 2, indicating B channels 1 and 2.
<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

## show interfaces serial bchannel

To display information about the physical attributes of the ISDN PRI over channelized E1 or channelized T1 B and D channels, use the **show interfaces serial bchannel** EXEC command.

```
show interfaces serial slot/port bchannel channel-number
```

```
show interfaces serial number bchannel channel-number
```

Syntax Description	
<i>slot/port</i>	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.
<i>number</i>	Network processor module (NPM) number, in the range 0 through 2.
<i>channel-number</i>	E1 channel number ranging from 1 to 31 or T1 channel number ranging from 1 to 23; 1 to 24 if using NFAS.

## show interfaces virtual-access

To display status, traffic data, and configuration information about a specified virtual access interface, use the **show interfaces virtual-access EXEC** command.

```
show interfaces virtual-access number [configuration]
```

---

### Syntax Description

---

*number*            Number of the virtual access interface.

---

**configuration**    (Optional) Restricts output to configuration information.

---

## show ip interface virtual-access

To display network layer IP information about a specified virtual access interface, use the **show ip interface virtual-access EXEC** command.

```
show ip interface virtual-access number
```

---

### Syntax Description

---

*number*            Number of the virtual access interface.

---

## show ip local pool

To display statistics for any defined IP address pools, use the **show ip local pool** privileged EXEC command.

```
show ip local pool [name]
```

---

### Syntax Description

---

*name*            (Optional) Name of a specific IP address pool.

---

## show ip route

To display all static IP routes or those installed using the authentication, authorization, and accounting (AAA) route download function, use the **show ip route EXEC** command.

```
show ip route [address [network-mask] [longer-prefixes]] | [protocol [process-id]] | [static
[download]]
```

---

### Syntax Description

---

*address*            (Optional) The IP address about which routing information should be displayed.

---

*network-mask*      (Optional) Network mask that lets you mask network and subnetwork bits.

---

**longer-prefixes**    (Optional) The *address* and *mask* pair becomes a prefix, and any routes that match that prefix are displayed.

---

<i>protocol</i>	(Optional) Name of a routing protocol; or the keyword <b>connected</b> , <b>static</b> , or <b>summary</b> . If you specify a routing protocol, use one of the following keywords: <b>bgp</b> , <b>egp</b> , <b>eigrp</b> , <b>hello</b> , <b>igrp</b> , <b>isis</b> , <b>ospf</b> , or <b>rip</b> .
<i>process-id</i>	(Optional) Arbitrary number assigned to identify a process of the specified protocol.
<b>static</b>	(Optional) All static routes.
<b>download</b>	(Optional) The route installed using the AAA route download function.

## show ipx compression

To show the current status and statistics of Internetwork Packet Exchange (IPX) header compression during PPP sessions, use the **show ipx compression EXEC** command.

```
show ipx compression [detail int-spec]
```

### Syntax Description

<b>detail</b>	(Optional) Displays detailed link-state database information for NLSP.
<i>int-spec</i>	(Optional) Interface type, as listed in Table 47.

**Table 47** Interface Types

Keyword	Description
<b>Async</b>	Asynchronous interface.
<b>Ethernet</b>	Ethernet IEEE 802.3 interface.
<b>Null</b>	Null interface.
<b>Serial</b>	WAN serial interface.

## show ipx spx-protocol

To view the status of the Sequenced Packet Exchange (SPX) protocol stack and related counters, use the **show ipx spx-protocol EXEC** command.

```
show ipx spx-protocol
```

### Syntax Description

This command has no arguments or keywords.

## show isdn

To display the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels, use the **show isdn** command in EXEC mode.

```
show isdn {active [dsl | serial number] | history [dsl | serial number] | memory | service [dsl |
serial number] | status [dsl | serial number] | timers [dsl | serial number]}
```

### Syntax Description

<b>active</b> [dsl   serial number]	Displays current call information of all ISDN interfaces or, optionally, a specific digital signal link (DSL) or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range 0 to 15. Information displayed includes the called number, the remote node name, the seconds of connect time, the seconds of connect time remaining, the seconds idle and AOC charging time units used during the call.
<b>history</b> [dsl   serial number]	Displays historic and current call information of all ISDN interfaces or, optionally, a specific digital signal link (DSL) or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range 0 to 15. Information displayed includes the called number, the remote node name, the seconds of connect time, the seconds of connect time remaining, the seconds idle and AOC charging time units used during the call.
<b>memory</b>	Displays ISDN memory pool statistics. This keyword is for use by technical development staff only.
<b>service</b> [dsl   serial number]	Displays the service status of all ISDN interfaces or, optionally, a specific digital signal link (DSL) or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range 0 to 15.
<b>status</b> [dsl   serial number]	Displays the status of all ISDN interfaces or, optionally, a specific digital signal link (DSL) or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range 0 to 15.
<b>timers</b> [dsl   serial number]	Displays the values of Layer 2 and Layer 3 timers for all ISDN interfaces or, optionally, a specific digital signal link (DSL) or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range 0 to 15.

## show isdn nfas group

To display all the members of a specified NFAS group or all NFAS groups, use the **show isdn nfas group** privileged EXEC command.

```
show isdn nfas group [number]
```

### Syntax Description

<i>number</i>	(Optional) Identifier number of a specific NFAS group.
---------------	--

## show isdn service

To display the service status of each ISDN channel, use the **show isdn service** privileged EXEC command.

```
show isdn service
```

---

**Syntax Description** This command has no arguments or keywords.

## show line async-queue

To display the status of connections currently waiting in the queue, use the **show line async-queue** EXEC command.

```
show line async-queue [rotary-group]
```

---

**Syntax Description** *rotary-group* (Optional) Specifies a rotary group.

---

## show modem

To display a high-level performance report for all the modems or a single modem inside Cisco access servers, use the **show modem** EXEC command.

```
show modem [slot/port | group number]
```

---

**Syntax Description** *slot/port* (Optional) Location of a slot and modem port. Remember to include the forward slash (/) when entering this variable.

---

*group number* (Optional) Modem group to which a specified modem belongs. The group number range is 1 to 200.

---

## show modem at-mode

To display a list of the manageable Microcom modems that have open AT sessions and a list of users logged in to those sessions, use the **show modem at-mode** EXEC command.

```
show modem at-mode
```

---

**Syntax Description** This command has no arguments or keywords.

## show modem call-stats

To display the local disconnect reasons for all modems inside an access server or router, use the **show modem call-stats** EXEC command.

```
show modem call-stats [slot]
```

<b>Syntax Description</b>	<i>slot</i>	(Optional) Slot number, which limits the display output to a particular range of modems in the system.
---------------------------	-------------	--

## show modem calltracker

To display all information stored within the Call Tracker active or history database for the latest call assigned to a specified modem, use the **show modem calltracker** privileged EXEC command. This command allows you to display all Call Tracker data for a given modem when you do not have the call handle readily available and do not want to search the Call Tracker database.

```
show modem calltracker [slot/port]
```

<b>Syntax Description</b>	<i>slot/port</i>	(Optional) Location of a slot and modem port. Remember to include the forward slash (/) when entering this argument.
---------------------------	------------------	--

## show modem configuration

To display the current modem configuration for digital MICA technologies modems loaded inside an access server or router, use the **show modem configuration** EXEC command.

```
show modem configuration [slot/port]
```

<b>Syntax Description</b>	<i>slot/port</i>	(Optional) Slot and modem port location. If this number is not specified, statistics for all connected modems are displayed. (Include the forward slash (/) when entering this argument.)
---------------------------	------------------	---

## show modem connect-speeds

To display connection speed statistics for all the modems running in an access server or router, use the **show modem connect-speeds** EXEC command.

```
show modem connect-speeds [max-speed [slot]]
```

<b>Syntax Description</b>	<i>max-speed</i>	(Optional) Maximum speed you want displayed in the shifting speed window. You can specify from 12,000 to 56,000 bps.
	<i>slot</i>	(Optional) Slot number, which limits the display output to a particular range of modems in the system.

## show modem cookie

To display information about the modem cookie, use the **show modem cookie** EXEC command.

```
show modem cookie
```

**Syntax Description** This command has no arguments or keywords.

## show modem csm

To display the internal status of the call switching module for modems inside access servers or routers, use the **show modem csm** EXEC command.

```
show modem csm [slot/port | group number]
```

<b>Syntax Description</b>	<i>slot/port</i>	(Optional) Slot and modem port location. If this number is not specified, statistics for all connected modems are displayed. (Include the forward slash (/) when entering this variable.)
	<i>group number</i>	(Optional) Specific group of modems. If the modem group number is not specified, statistics for all modems in the access server are displayed. The group number range is between 1 and 200.

## show modem log

To display the modem history event status performed on a manageable modem or group of modems, use the **show modem log** EXEC command.

```
show modem log [slot/port | group number]
```

<b>Syntax Description</b>	<i>slot/port</i>	(Optional) Slot and modem port location. If this number is not specified, statistics for all connected modems are displayed. (Include the forward slash (/) when entering this variable.)
	<i>group number</i>	(Optional) Specific group of modems. If the modem group number is not specified, statistics for all modems in the access server are displayed. The group number range is between 1 and 200.

## show modem mapping

To display a snapshot of all the firmware versions running on all the modems in the access server, use the **show modem mapping** EXEC command.

```
show modem mapping
```

---

**Syntax Description** This command has no arguments or keywords.

## show modem mica

To display information about MICA digital modems, use the **show modem mica** EXEC command.

```
show modem mica {slot/port | all | slot [number]}
```

---

<b>Syntax Description</b>	<i>slot/port</i>	Single modem in a MICA digital modem board.
	<b>all</b>	All the MICA modems in the system.
	<b>slot number</b>	A particular slot, which is mainly used for debugging purposes. The optional <i>number</i> argument allows you to specify a slot number.

---

## show modem operational-status

To display performance statistics for individual modems, use the **show modem operational-status** EXEC command.

```
show modem operational-status [slot/port]
```

---

<b>Syntax Description</b>	<i>shelf/slot/port</i>	(Optional) Location of the slot and modem port. If these numbers are not specified, statistics for all connected modems are displayed. (Include the forward slash (/) when entering these arguments.)
---------------------------	------------------------	---

---

## show modem-pool

To display the configuration and connection status for one or more modem pools, use the **show modem-pool** EXEC command.

```
show modem-pool [name]
```

---

<b>Syntax Description</b>	<i>name</i>	(Optional) Modem pool name.
---------------------------	-------------	-----------------------------

---

## show modem summary

To display a high-level report for all manageable modems dialing in to and out of the network, use the **show modem summary** EXEC command.

```
show modem summary
```

---

**Syntax Description** This command has no arguments or keywords.

## show modem test

To display the modem test log, use the **show modem test** EXEC command.

```
show modem test
```

---

**Syntax Description** This command has no arguments or keywords.

## show modem version

To display version information about the modem firmware, controller and Domain Specific Part—ATM address field (DSP) code (for 56K modems only), and boot code, use the **show modem version** EXEC command.

```
show modem version
```

---

**Syntax Description** This command has no arguments or keywords.

## show modemcap

To display the values set for the current modem and list the modems for which the router has entries, use the **show modemcap** EXEC command. To display the attributes associated with a specific modem, use the **show modemcap** EXEC command with the optional *modem-name* argument.

```
show modemcap [modem-name]
```

---

**Syntax Description** *modem-name* (Optional) Name of the modem (such as Codex\_3260).

---

## show nbf cache

To display NetBIOS name cache contents, use the **show nbf cache** EXEC command.

```
show nbf cache
```

---

**Syntax Description** This command has no arguments or keywords.

## show nbf sessions

To view NetBEUI connection information, use the **show nbf sessions** EXEC command.

```
show nbf sessions
```

---

**Syntax Description** This command has no arguments or keywords.

## show port config

To display the active session's configuration parameters, use the **show port config** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show port config {slot | slot/port}
```

### Cisco AS5800 with Universal Port Card

```
show port config {shelf/slot | shelf/slot/port}
```

---

<b>Syntax Description</b>	<i>slot</i>	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/port</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
	<i>shelf/slot</i>	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/port</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

---

## show port digital log

To display the data event log for digital modems, use the **show port digital log** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show port digital log [reverse slot/port] [slot | slot/port]
```



#### Note

This command is not supported on the Cisco AS5800 with the universal port card.

#### Syntax Description

<b>reverse</b>	(Optional) Report displayed with most recent entry first.
<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/port</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.

## show port modem calltracker

To display the port-level information for an active modem, use the **show port modem calltracker** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show port modem calltracker [slot | slot/port]
```

### Cisco AS5800 with universal port card

```
show port modem calltracker [shelf/slot | shelf/slot/port]
```

#### Syntax Description

<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/port</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
<i>shelf/slot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
<i>shelf/slot/port</i>	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

## show port modem log

To display the events generated by the modem sessions, use the **show port modem log EXEC** command.

### Cisco AS5400 with NextPort DFC

```
show port modem log [reverse slot/port] [slot | slot/port]
```

### Cisco AS5800 with Universal Port Card

```
show port modem log [reverse shelf/slot/port] [shelf/slot | shelf/slot/port]
```

Syntax Description	reverse	(Optional) Displays the modem port history event log with the most recent event first.
	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/port</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
	<i>shelf/slot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/port</i>	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

## show port modem test

To display the modem test log, use the **show port modem test EXEC** command.

### Cisco AS5400 with NextPort DFC

```
show port modem test [slot | slot/port]
```

### Cisco AS5800 with Universal Port Card

```
show port modem test [shelf/slot | shelf/slot/port]
```

	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/port</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
	<i>shelf/slot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/port</i>	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

## show port operational-status

To display the active session's statistics, use the **show port operational-status** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show port operational-status {slot | slot/port}
```

### Cisco AS5800 with Universal Port Card

```
show port operational-status {shelf/slot | shelf/slot/port}
```

Syntax Description	slot	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	slot/port	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.
	shelf/slot	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	shelf/slot/port	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.

## show ppp bap

To display the configuration settings and run-time status for a multilink bundle, use the **show ppp bap** privileged EXEC command.

```
show ppp bap {group [name] | queues}
```

Syntax Description	group [name]	All or, optionally, a specific BACP bundle group.
	queues	BACP queues.

## show ppp mppe

To display Microsoft Point-to-Point Encryption (MPPE) information for an interface, use the **show ppp mppe** privileged EXEC command.

```
show ppp mppe {serial | virtual-access}[number]
```

Syntax Description	serial	Displays MPPE information for all serial interfaces.
	virtual-access	Displays MPPE information for all virtual-access interfaces.
	number	(Optional) Displays MPPE information for only the specified interface.

## show ppp multilink

To display bundle information for the Multilink PPP bundles, use the **show ppp multilink** EXEC command.

```
show ppp multilink
```

---

**Syntax Description** This command has no arguments or keywords.

## show queuing virtual-access

To display information about interleaving, use the **show queuing virtual-access** EXEC command.

```
show queuing virtual-access number
```

---

**Syntax Description** *number* Virtual access interface number.

---

## show rcapi status

To display whether RCAP is turned on or off, use the **show rcapi status** privileged EXEC command.

```
show rcapi status
```

---

**Syntax Description** This command has no arguments or keywords.

## show redundancy

To display current or historical status and related information on redundant Dial Shelf Controller (DSC), use the **show redundancy** privileged EXEC command.

```
show redundancy [history]
```

---

**Syntax Description** **history** (Optional) Past status and related information on the redundant DSCs.

---

## show resource-pool call

To display all active call information for all customer profiles and resource groups, use the **show resource-pool call** EXEC command.

```
show resource-pool call
```

---

**Syntax Description** This command has no arguments or keywords.

## show resource-pool customer

To display the contents of one or more customer profiles, use the **show resource-pool customer** EXEC command.

```
show resource-pool customer [name]
```

---

**Syntax Description** *name* (Optional) Name of a specific customer profile. The name can have up to 23 characters.

---

## show resource-pool discriminator

To see how many times an incoming call has been rejected due to a specific Calling Line Identification (CLID) or Dialed Number Identification Service (DNIS) call-type combination, use the **show resource-pool discriminator** user and privileged EXEC command.

```
show resource-pool discriminator [name]
```

---

**Syntax Description** *name* (Optional) Name of the specific CLID or DNIS and call-type that will be rejected. The name can have up to 23 characters.

---

## show resource-pool resource

To see the resource groups configured in the network access server, use the **show resource-pool resource** EXEC command.

```
show resource-pool resource [name]
```

---

**Syntax Description** *name* (Optional) Contents of a specifically named resource group, which was set up by using the **resource-pool group resource** *name* command. The name can have up to 23 characters.

---

## show resource-pool vpdn

To see the contents of a specific virtual private dial-up network (VPDN) group or specific VPDN profile, use the **show resource-pool vpdn** EXEC command.

```
show resource-pool vpdn {group | profile} [name]
```

---

### Syntax Description

<b>group</b>	All the VPDN groups configured inside the network access server.
<b>profile</b>	All the VPDN profiles configured inside the network access server.
<i>name</i>	(Optional) Specific VPDN group or profile.

---

## show rlm group statistics

To display the network latency of the Redundant Link Manager (RLM) group, use the **show rlm group statistics** privileged EXEC command.

```
show rlm group group-number statistics
```

---

### Syntax Description

<i>group-number</i>	RLM group number (0 to 255).
---------------------	------------------------------

---

## show rlm group status

To display the status of the Redundant Link Manager (RLM) group, use the **show rlm group status** privileged EXEC command.

```
show rlm group group-number status
```

---

### Syntax Description

<i>group-number</i>	RLM group number (0 to 255).
---------------------	------------------------------

---

## show rlm group timer

To display the current timer values, use the **show rlm group timer** privileged EXEC command.

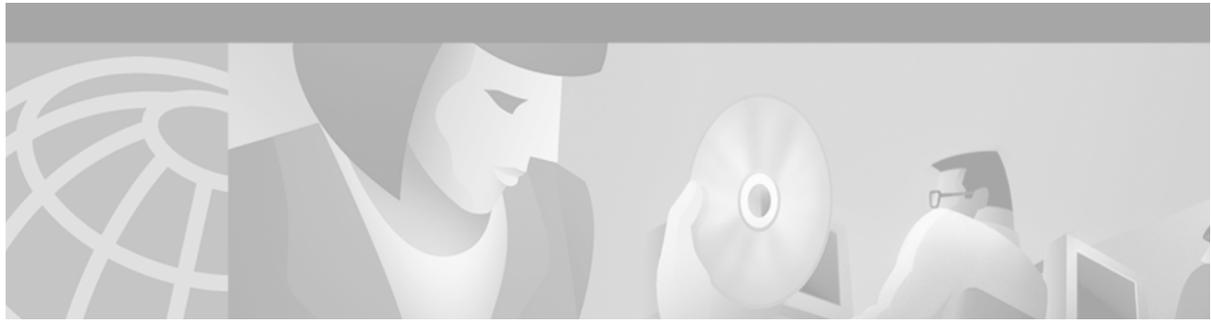
```
show rlm group group-number timer
```

---

### Syntax Description

<i>group-number</i>	RLM group number (0 to 255).
---------------------	------------------------------

---



## Dial Technologies Commands: show sessions Through x25 map ppp

---

This chapter describes the function and syntax of the dial technologies commands: **show sessions** through **x25 map ppp**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Dial Technologies Command Reference*.

### show sessions

To display information about open local-area transport (LAT), Telnet, or rlogin connections, use the **show sessions** EXEC command.

```
show sessions
```

---

**Syntax Description** This command has no arguments or keywords.

### show sgbp

To display the status of the stack group members, use the **show sgbp** EXEC command.

```
show sgbp
```

---

**Syntax Description** This command has no arguments or keywords.

### show sgbp queries

To display the current seed bid value, use the **show sgbp queries** EXEC command.

```
show sgbp queries
```

---

**Syntax Description** This command has no arguments or keywords.

## show snapshot

To display snapshot routing parameters associated with an interface, use the **show snapshot** EXEC command.

```
show snapshot [interface-type interface-number]
```

---

### Syntax Description

<i>interface-type</i>	(Optional) Interface type and number.
<i>interface-number</i>	

---

## show spe

To show Service Processing Element (SPE) status, use the **show spe** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe [slot | slot/spe]
```

### Cisco AS5800 with Universal Port Card

```
show spe [shelf/slot | shelf/slot/spe]
```

---

### Syntax Description

<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/spe</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
<i>shelf/slot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
<i>shelf/slot/spe</i>	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

---

## show spe digital

To display history statistics of all digital Service Processing Elements (SPEs), in summary form or for SPEs starting with a specified slot or a specified shelf/slot/range of SPEs, use the **show spe digital** EXEC command.

```
show spe digital [slot | slot/spe]
```



### Note

---

This command is not supported on the Cisco AS5800 with the universal port card.

---

<b>Syntax Description</b>	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.

## show spe digital active

To display active digital calls and digital statistics of all Service Processing Elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital active** EXEC command.

```
show spe digital active [slot | slot/spe]
```



### Note

This command is not supported on the Cisco AS5800 with the universal port card.

<b>Syntax Description</b>	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.

## show spe digital csr

To display digital calls success rate (CSR) statistics of all Service Processing Elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital csr** EXEC command.

```
show spe digital csr [summary | slot | slot/spe]
```



### Note

This command is not supported on the Cisco AS5800 with the universal port card.

<b>Syntax Description</b>	<b>summary</b>	(Optional) Summary digital CSR statistics.
	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.

## show spe digital disconnect-reason

To display the local disconnect reasons for all digital calls on the Service Processing Elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital disconnect-reason** EXEC command.

```
show spe digital disconnect-reason [summary | slot | slot/spe]
```



### Note

This command is not supported on the Cisco AS5800 with the universal port card.

### Syntax Description

<b>summary</b>	(Optional) Summary of local disconnect reasons for digital ports.
<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/spe</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.

## show spe digital summary

To display history statistics of all Service Processing Elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital summary** EXEC command.

```
show spe digital summary [slot | slot/spe]
```



### Note

This command is not supported on the Cisco AS5800 with the universal port card.

### Syntax Description

<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/spe</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.

## show spe log

To display the Service Processing Element (SPE) system log, use the **show spe log** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe log [reverse | slot]
```

### Cisco AS5800 with Universal Port Card

```
show spe log [reverse | shelf/slot]
```

Syntax Description		
<b>reverse</b>	(Optional)	Displays the SPE system log with the most recent event first.
<i>slot</i>	(Optional)	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>shelf/slot</i>	(Optional)	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.

## show spe modem

To display the modem service history statistics for a specified Service Processing Element (SPE), use the **show spe modem** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe modem {slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem {shelf/slot | shelf/slot/spe}
```

Syntax Description		
<i>slot</i>	(Optional)	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/spe</i>	(Optional)	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
<i>shelf/slot</i>	(Optional)	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
<i>shelf/slot/spe</i>	(Optional)	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem active

To display statistics of all active calls on specified Service Processing Elements (SPEs), use the **show spe modem active** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe modem active {slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem active {shelf/slot | shelf/slot/spe}
```

Syntax Description		
<i>slot</i>		All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/spe</i>		All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
<i>shelf/slot</i>		All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
<i>shelf/slot/spe</i>		All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem csr

To display the call success rate for the specified Service Processing Elements (SPEs), use the **show spe modem csr** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe modem csr {summary | slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem csr {summary | shelf/slot | shelf/slot/spe}
```

Syntax Description		
<b>summary</b>		Displays all call success rate statistics for all SPEs.
<i>slot</i>		All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
<i>slot/spe</i>		All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
<i>shelf/slot</i>		All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
<i>shelf/slot/spe</i>		All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem disconnect-reason

To display all modem disconnect reasons for the specified Service Processing Element (SPE), use the **show spe modem disconnect-reason** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe modem disconnect-reason {summary | slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem disconnect-reason {summary | shelf/slot | shelf/slot/spe}
```

Syntax Description	summary	Displays the disconnect reasons for all SPEs.
	<i>slot</i>	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	<i>shelf/slot</i>	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/spe</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem high speed

To display the total number of connections within each high-speed modulation or codec for a specific range of Service Processing Elements (SPEs), use the **show spe modem high speed** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe modem high speed {summary | slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem high speed {summary | shelf/slot | shelf/slot/spe}
```

Syntax Description	summary	Displays a brief list of all modulation connections negotiated.
	<i>slot</i>	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	<i>shelf/slot</i>	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/spe</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem high standard

To display the total number of connections within each high modulation or codec for a specific range of Service Processing Element (SPE), use the **show spe modem high standard** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe modem high standard {summary | slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem high standard {summary | shelf/slot | shelf/slot/spe}
```

Syntax Description	summary	Displays a brief list of all modulation connections negotiated.
	<i>slot</i>	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	<i>shelf/slot</i>	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/spe</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem low speed

To display the connect speeds within each low-speed modulation or codec for the specified Service Processing Elements (SPEs), use the **show spe modem low speed EXEC** command.

### Cisco AS5400 with NextPort DFC

```
show spe modem low speed {summary | slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem low speed {summary | shelf/slot | shelf/slot/spe}
```

Syntax Description	summary	Displays a brief list of all modulation connections negotiated.
	<i>slot</i>	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	Ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7; SPE values range from 0 to 17.
	<i>shelf/slot</i>	Ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/spe</i>	Ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem low standard

To display the total number of connections within each low modulation or codec for the specified Service Processing Elements (SPEs), use the **show spe modem low standard EXEC** command.

### Cisco AS5400 with NextPort DFC

```
show spe modem low standard {summary | slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
show spe modem low standard {summary | shelf/slot | shelf/slot/spe}
```

Syntax Description	summary	Displays a brief list of all modulation connections negotiated.
	<i>slot</i>	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	<i>shelf/slot</i>	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/spe</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe modem summary

To display summary of modem statistics for the specified Service Processing Element (SPE) or range of SPEs, use the **show spe modem summary** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe modem summary [slot | slot/spe]
```

### Cisco AS5800 with Universal Port Card

```
show spe modem summary [shelf/slot | shelf/slot/spe]
```

Syntax Description	<i>slot</i>	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	<i>slot/spe</i>	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	<i>shelf/slot</i>	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	<i>shelf/slot/spe</i>	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe recovery

To display SPE recovery statistics, use the **show spe recovery** EXEC command.

### Cisco AS5400 with NextPort DFC

```
show spe recovery [slot | slot/spe]
```

### Cisco AS5800 with Universal Port Card

```
show spe recovery [shelf/slot | shelf/slot/spe]
```

Syntax Description	slot	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	slot/spe	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	shelf/slot	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	shelf/slot/spe	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show spe version

To display the firmware version on a Service Processing Element (SPE), use the **show spe version EXEC** command.

### Cisco AS5400 with NextPort DFC

```
show spe version [slot | slot/spe]
```

### Cisco AS5800 with Universal Port Card

```
show spe version [shelf/slot | shelf/slot/spe]
```

Syntax Description	slot	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	slot/spe	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	shelf/slot	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	shelf/slot/spe	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## show tgrm

To display information for debugging purposes about defined trunk groups and interfaces that have been assigned to the trunk groups, use the **show tgrm EXEC** command.

```
show tgrm
```

**Syntax Description** This command has no arguments or keywords.

## show vpdn

To display information about active Level 2 Forwarding (L2F) Protocol tunnel and message identifiers in a virtual private dialup network (VPDN), use the **show vpdn** EXEC command.

```
show vpdn [session][packets][tunnel][all]
```

Syntax Description	session	(Optional) Displays a summary of the status of all active tunnels.
	packets	(Optional) Displays a summary of packets coming in and going out of a session.
	tunnel	(Optional) Displays information about all active L2F and L2TP tunnels in summary-style format.
	all	(Optional) Displays summary information about all active L2F and L2TP tunnels.

## show vpdn domain

To view all virtual private dialup network (VPDN) domains and DNIS groups configured on the network access server, use the **show vpdn domain** privileged EXEC command.

```
show vpdn domain
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

## show vpdn group

To see a summary of the relationships among virtual private dialup network (VPDN) groups and customer/VPDN profiles, or to summarize the configuration of a VPDN group including domain/DNIS, load sharing information and current session information, use the **show vpdn group** EXEC command.

```
show vpdn group [name] [domain | endpoint]
```

Syntax Description	name	(Optional) VPDN group name summarizes the configuration of the specified group.
	domain	(Optional) DNIS/domain information.
	endpoint	(Optional) Endpoint session information.

## show vpdn history failure

To show the content of the failure history table, use the **show vpdn history failure** EXEC command.

```
show vpdn history failure [user-name]
```

<b>Syntax Description</b>	<i>user-name</i>	(Optional) Username, which displays only the entries mapped to that particular user.
---------------------------	------------------	--

## show vpdn multilink

To see the multilink sessions authorized for all virtual private dialup network (VPDN) groups, use the **show vpdn multilink** EXEC command.

```
show vpdn multilink
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## shutdown (RLM)

To shut down all of the links under the RLM group, use the **shutdown** command. RLM will not try to reestablish those links until the command is negated. To disable this function, use the **no** form of this command.

```
shutdown
```

```
no shutdown
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## shutdown (port)

To disable a port, use the **shutdown** port configuration command. To change the administrative state of a port from out-of-service to in service, use the **no** form of this command.

```
shutdown
```

```
no shutdown
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## shutdown (spe)

To take a Service Processing Element (SPE) out of service, use the **shutdown** SPE configuration command. To change the administrative state of this SPE from down to up, use the **no** form of this command.

**shutdown**

**no shutdown**

---

**Syntax Description** This command has no arguments or keywords.

## signaling-class cas

To define a signalling class with a template formed by directives guiding the Call Service Module (CSM) to process the digit sequence, use the **signaling-class cas** global configuration command. To remove the signalling class assignment, use the **no** form of this command.

**signaling-class cas** *name*

**no signaling-class cas** *name*

---

**Syntax Description**

<i>name</i>	The signalling class name, which specifies the template that processes the ANI/DNIS delimiter.
-------------	--

---

## snapshot client

To configure a client router for snapshot routing, use the **snapshot client** interface configuration command. To disable a client router, use the **no** form of this command.

**snapshot client** *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

**no snapshot client** *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

---

**Syntax Description**

<i>active-time</i>	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value is 5 minutes.
<i>quiet-time</i>	Amount of time, in minutes, that routing entries are frozen and remain unchanged between active periods. Routes are not aged during the quiet period, so they remain in the routing table as if they were static entries. This argument can be an integer from 8 to 100000. There is no default value. The minimum quiet time is generally the active time plus 3.

---

<b>suppress-statechange-updates</b>	(Optional) Disables the exchange of routing updates each time the line protocol goes from “down” to “up” or from “dialer spoofing” to “fully up.”
<b>dialer</b>	(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

## snapshot server

To configure a server router for snapshot routing, use the **snapshot server** interface configuration command. To disable a server router, use the **no** form of this command.

**snapshot server** *active-time* [**dialer**]

**no snapshot server** *active-time* [**dialer**]

<b>Syntax Description</b>	<i>active-time</i>	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value is 5 minutes.
	<b>dialer</b>	(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

## source template

To attach a configured customer profile template to a particular customer profile, use the **source template** customer profile configuration command.

**source template** *name*

<b>Syntax Description</b>	<i>name</i>	Customer profile template name.
---------------------------	-------------	---------------------------------

## source-ip

To specify an alternate IP address for a virtual private dialup network (VPDN) tunnel that is different from the physical IP address used to open the tunnel, use the **source-ip** group configuration command. To remove the alternate IP address, use the **no** form of this command.

**source-ip** *ip-address*

**no source-ip**

<b>Syntax Description</b>	<i>ip-address</i>	Alternate IP address (different from the physical IP address used to open the VPDN tunnel) that the router uses to identify the tunnel.
---------------------------	-------------------	---

## spe

To enter Service Processing Element (SPE) configuration mode and set the range of SPEs, use the **spe** global configuration command.

### Cisco AS5400 with NextPort DFC

```
spe {slot | slot/spe}
```

### Cisco AS5800 with Universal Port Card

```
spe {shelf/slot | shelf/slot/spe}
```

Syntax Description	slot	All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
	slot/spe	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and SPE values range from 0 to 17.
	shelf/slot	All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11.
	shelf/slot/spe	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53.

## spe call-record modem

To generate a modem call record at the end of each call, use the **spe call-record modem** global configuration command. To cancel the request to generate the reports, use the **no** form of the command.

```
spe call-record modem {max-userid number | quiet}
```

```
no spe call-record modem {max-userid number | quiet}
```

Syntax Description	max-userid number	Maximum length of User ID for the modem call record report in number of bytes. The range is 0 to 100.
	quiet	Disables logging to console and terminal, but not to syslog.

## spe country

To specify the country while setting the Universal Port DFC parameters (including country code and encoding), use the **spe country** global configuration command. To set the country code to the default value, use the **no** form of this command.

```
spe country country-name
```

```
no spe country country-name
```

Syntax Description	country-name	Name of the country; see Table 48 for a list of supported country name keywords.
--------------------	--------------	--

**Table 48 Country Names and Corresponding Companding Law**

<b>Keyword</b>	<b>Country</b>	<b>Companding Law</b>
<b>australia</b>	Australia	a-law
<b>austria</b>	Austria	a-law
<b>belgium</b>	Belgium	a-law
<b>china</b>	China	a-law
<b>cyprus</b>	Cyprus	a-law
<b>czech-republic</b>	Czech/Slovak Republic	a-law
<b>denamrk</b>	Denmark	a-law
<b>e1-default</b>	Default for E-1	a-law
<b>finland</b>	Finland	a-law
<b>france</b>	France	a-law
<b>germany</b>	Germany	a-law
<b>hong-kong</b>	Hong Kong	u-law
<b>india</b>	India	a-law
<b>ireland</b>	Ireland	a-law
<b>israel</b>	Israel	a-law
<b>italy</b>	Italy	a-law
<b>japan</b>	Japan	u-law
<b>malaysia</b>	Malaysia	a-law
<b>netherlands</b>	Netherlands	a-law
<b>new-zealand</b>	New Zealand	a-law
<b>norway</b>	Norway	a-law
<b>poland</b>	Poland	a-law
<b>portugal</b>	Portugal	a-law
<b>russia</b>	Russia	a-law
<b>singapore</b>	Singapore	a-law
<b>south-africa</b>	South Africa	a-law
<b>spain</b>	Spain	a-law
<b>sweden</b>	Sweden	a-law
<b>switzerland</b>	Switzerland	a-law
<b>t1-default</b>	Default for T1	u-law
<b>taiwan</b>	Taiwan	u-law
<b>thailand</b>	Thailand	a-law
<b>turkey</b>	Turkey	a-law
<b>united-kingdom</b>	United Kingdom	a-law
<b>usa</b>	United States of America	u-law

## spe download maintenance

To perform download maintenance on Service Processing Elements (SPEs) that are marked for recovery, use the **spe download maintenance** global configuration command. To unmark the ports, use the **no** form of the command.

```
spe download maintenance {time hh:mm | stop-time hh:mm | max-spes num-of-spes | window
time-period | expired-window {drop-call | reschedule}}
```

```
no spe download maintenance {time hh:mm | stop-time hh:mm | max-spes num-of-spes | window
time-period | expired-window {drop-call | reschedule}}
```

Syntax Description		
<b>time</b> <i>hh:mm</i>		Time of the day to start the download maintenance activity. Enter the value in the format of the variable as shown. Default is 03:00 a.m.
<b>stop-time</b> <i>hh:mm</i>		Time of the day to stop the download maintenance activity. Enter the value in the format of the variable as shown.
<b>max-spes</b> <i>num-of-spes</i>		Maximum number of SPEs that can simultaneously be in maintenance. The value is between 1 and 10,000. Default is equal to 20 percent of the maximum number of SPEs in each NextPort DFC.
<b>window</b> <i>time-period</i>		Time window to perform the maintenance activity. The value is between 0 and 360 minutes. Default is 60 minutes.
<b>expired-window</b>		Action to take if SPE maintenance is not completed within the specified window. Default is <b>reschedule</b> .
<b>drop-call</b>		Expired window choice that forces download by dropping active calls.
<b>reschedule</b>		Expired window choice that defers recovery to the next maintenance time (default for <b>expired-window</b> keyword).

## spe log-event-size

To set the maximum size of the history event queue for log entries for each port, use the **spe log-event-size** global configuration command.

```
spe log-event-size number
```

Syntax Description		
<i>number</i>		Number of recorded events. The number range is 0 to 100.

## spe recovery

To set a Service Processing Element (SPE) port for recovery, use the **spe recovery** global configuration command.

```
spe recovery {port-action {disable | recover} | {port-threshold num-failures}}
```

Syntax Description		
<b>port-action</b>		Action to apply to the port for recovery. Default is <b>none</b> .
<b>disable</b>		Sets port in a Bad state.
<b>recover</b>		Sets port for recovery.
<b>port-threshold</b> <i>num-failures</i>		Number of consecutive failed attempts made on the port before applying <b>port-action</b> . Enter an integer value. The range is from 1 to 1000. Default is 30 consecutive call failures.

## start-character

To set the flow control start character, use the **start-character** line configuration command. To remove the character, use the **no** form of this command.

**start-character** *ascii-number*

**no start-character**

Syntax Description	<i>ascii-number</i>	Decimal representation of the start character.
--------------------	---------------------	--

## start-chat

To specify that a chat script start on a specified line at any point, use the **start-chat** privileged EXEC command. To stop the chat script, use the **no** form of this command.

**start-chat** *regexp* [*line-number* [*dialer-string*]]

**no start-chat**

Syntax Description	<i>regexp</i>	Name of a regular expression or modem script to be executed. If there is more than one script with a name that matches the argument <i>regexp</i> , the first script found will be used.
	<i>line-number</i>	(Optional) Line number on which to execute the chat script. If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the dialer-string argument is specified, line-number must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal (VTY) lines.
	<i>dialer-string</i>	(Optional) String of characters (often a telephone number) to be sent to a DCE. If you enter a dialer string, you must also specify <i>line-number</i> , or the chat script <i>regexp</i> will not start.

## stop-character

To set the flow control stop character, use the **stop-character** line configuration command. To remove the character, use the **no** form of this command.

**stop-character** *ascii-number*

**no stop-character**

---

### Syntax Description

<i>ascii-number</i>	Decimal representation of the stop character.
---------------------	---

---

## template

To access the template configuration mode for configuring a particular customer profile template, use the **template** global configuration command. To delete the template of the specified name, use the **no** form of this command.

**template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]

**no template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]

---

### Syntax Description

<i>name</i>	Identifies the template.
<b>default</b>	(Optional) Sets the command to its defaults.
<b>exit</b>	(Optional) Exits from resource-manager configuration mode.
<b>multilink</b>	(Optional) Configures multilink parameters.
<b>no</b>	(Optional) Negates the command or its defaults.
<b>peer</b>	(Optional) Accesses peer parameters for point-to-point interfaces.
<b>ppp</b>	(Optional) Accesses Point-to-Point Protocol.

---

## terminate-from

To specify the host name of the remote L2TP access concentrator (LAC) or L2TP network server (LNS) that will be required when accepting a virtual private dialup network (VPDN) tunnel, use the **terminate-from** VPDN group configuration command. To remove the host name from the VPDN group, use the **no** form of this command.

**terminate-from** **hostname** *host-name*

**no terminate-from** [**hostname** *host-name*]

---

### Syntax Description

<b>hostname</b> <i>host-name</i>	The host name that this VPDN group will accept connections from.
----------------------------------	--

---

## test modem back-to-back

To diagnose an integrated modem that may not be functioning properly, use the **test modem back-to-back** EXEC command.

```
test modem back-to-back first-slot/port second-slot/port
```

Syntax Description		
<i>first-slot/port</i>	Slot and modem number of the first test modem. (Include the forward slash (/) when entering this variable.)	
<i>second-slot/port</i>	Slot and modem number of the second test modem. (Include the forward slash (/) when entering this variable.)	

## test port modem back-to-back

To test two specified ports back-to-back and transfer a specified amount of data between the ports, use the **test port modem back-to-back** EXEC command.

### Cisco AS5400 with NextPort DFC

```
test port modem back-to-back {slot/port}
```

### Cisco AS5800 with Universal Port Card

```
test port modem back-to-back {shelf/slot/port}
```

Syntax Description		
<i>slot/port</i>	All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107.	
<i>shelf/slot/port</i>	All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323.	

## timer

To set the Redundant Link Manager (RLM) timer, use the **timer** RLM configuration command. The associated options can overwrite the default setting of timeout values. To disable this function, use the **no** form of this command.

```
timer {force-down | keepalive | minimum-up | open-wait | recovery | retransmit | switch-link}  
seconds
```

```
no timer {force-down | keepalive | minimum-up | open-wait | recovery | retransmit |  
switch-link} seconds
```

**Syntax Description**

<b>force-down</b>	After RLM enters the down state, RLM will stay in the down state for a certain amount of time to make sure that the remote end will also enter the down state. After this occurs, both can be forced to be in sync again. This timer can also prevent RLM links from going up and down rapidly in an unstable network environment.
<b>keepalive</b>	A keepalive packet will be sent out from Network Access Server (NAS) to CSC periodically.
<b>minimum-up</b>	After a link is recovered from the failure state and RLM is in the up state, RLM will wait for a minimum time to make sure the new recovered link is stabilized before doing any operation.
<b>open-wait</b>	To overcome the latency while opening several links at the same time, RLM will use this timer to wait before opening the new links, and then choose the link with the highest weighting to become the active signalling link.
<b>recovery</b>	When the network access server (NAS) loses the active connection to CSC, it will try to reestablish the connection within the interval specified by this command. If it fails to reestablish the connection, RLM will declare that the RLM signalling link is down.
<b>retransmit</b>	Because RLM is operating under UDP, it needs to retransmit the control packet if the packet is not acknowledged within this retransmit interval.
<i>seconds</i>	Time, in seconds, before executing the designated function.
<b>switch-link</b>	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM will go into the recovery state.

## trunk group (global)

To define a trunk group, use the **trunk group** global configuration command. To disable the specified trunk group, use the **no** form of this command.

```
trunk group group-number [max-calls { any | voice | data } number] [direction in | out]
[max-retries retries]
```

```
no trunk group group-number
```

**Syntax Description**

<i>group-number</i>	Identifier for this trunk group, in the range 1 to 1000.
<b>max-calls</b> [ <b>any</b>   <b>voice</b>   <b>data</b> ] <i>number</i>	(Optional) Specifies the maximum number of voice or data calls allowed on this trunk group or the maximum number of any type of calls allowed on this trunk group, in the range 1 to 1000.
<b>direction in</b>   <b>out</b>	(Optional) Specifies whether the trunk group is restricted to incoming or outgoing calls.
<b>max-retries</b> <i>retries</i>	(Optional) Specifies the maximum number of outgoing call attempts when a glare situation is encountered, in the range 1 to 5. The default value is the number of interfaces that belong to the trunk group

## trunk-group (interface)

To assign a specified PRI interface to a defined trunk group, use the **trunk-group** interface configuration command. To remove the specified interface from the defined trunk group, use the **no** form of this command.

**trunk-group** *group-number*

**no trunk-group** *group-number*

Syntax Description	<i>group-number</i>	The defined trunk group to which this PRI interface is assigned.
--------------------	---------------------	--

## trunkgroup (dial-peer)

To specify the trunk group to use for the configured dial peer, use the **trunkgroup** dial-peer configuration command. To remove the configured dial peer from the trunk group, use the **no** form of this command.

**trunkgroup** *group-number*

**no trunkgroup** *group-number*

Syntax Description	<i>group-number</i>	The trunk group to which this dial peer belongs.
--------------------	---------------------	--

## tunnel

To set up a network layer connection to a router, use the **tunnel** user EXEC command.

**tunnel** *host*

Syntax Description	<i>host</i>	Name or IP address of a specific host on a network that can be reached by the router.
--------------------	-------------	---

## virtual-profile aaa

To enable virtual profiles by authentication, authorization, and accounting (AAA) configuration, use the **virtual-profile aaa** global configuration command. To disable virtual profiles, use the **no** form of this command.

**virtual-profile aaa**

**no virtual-profile aaa**

Syntax Description	This command has no arguments or keywords.
--------------------	--

## virtual-profile if-needed

To specify that a virtual profile be used to create a virtual access interface only if the inbound connection requires a virtual access interface, use the **virtual-profile if-needed** global configuration command. To create virtual access interfaces for every inbound connection, use the **no** form of this command.

**virtual-profile if-needed**

**no virtual-profile if-needed**

---

**Syntax Description** This command has no arguments or keywords.

## virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** global configuration command. To disable this function, use the **no** form of this command.

**virtual-profile virtual-template** *number*

**no virtual-profile virtual-template** *number*

---

**Syntax Description** *number* Number of the virtual template to apply, in the range 1 to 30.

---

## virtual-template

To specify which virtual template will be used to clone virtual access interfaces, use the **virtual-template** accept-dialin configuration command. To remove the virtual template from an accept-dialin virtual private dialup network (VPDN) subgroup, use the **no** form of this command.

**virtual-template** *template-number*

**no virtual-template**

---

**Syntax Description** *template-number* Number of the virtual template that will be used to clone virtual-access interfaces.

---

## vpdn aaa attribute

To enable AAA attributes which are related to VPDN and will be reported to the AAA server in accounting records, use the **vpdn aaa attribute** global configuration command.

**vpdn aaa attribute** [**nas-ip-address nas-port** | **vpdn-nas vpdn-nas-port-ip-address**]

Syntax Description		
	<b>nas-ip-address</b>	(Optional) NAS IP address.
	<b>nas-port</b>	(Optional) NAS port.
	<b>vpdn-nas</b>	(Optional) VPDN NAS IP address
	<b>vpdn-nas-port-ip-address</b>	(Optional) VPDN NAS port.

## vpdn aaa override-server

To specify the AAA server to be used for VPDN tunnel authorization, use the **vpdn aaa override-server** global configuration command.

```
vpdn aaa override-server aaa-server-ip-address
```

Syntax Description		
	<i>aaa-server-ip-address</i>	Specify the IP address of the AAA server to be used for tunnel authorization.

## vpdn domain-delimiter

To specify the characters to be used to delimit the domain prefix or domain suffix, use the **vpdn domain-delimiter** global configuration command. To disable this function, use the **no** form of this command.

```
vpdn domain-delimiter characters [suffix | prefix]
```

```
no vpdn domain-delimiter characters [suffix | prefix]
```

Syntax Description		
	<i>characters</i>	One or more specific characters to be used as suffix or prefix delimiters. Available characters are %, -, @, \, #, and /.  If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).
	<b>suffix</b>   <b>prefix</b>	(Optional) Usage of the specified characters.

## vpdn enable

To enable virtual private dialup networking on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** global configuration command. To disable, use the **no** form of this command.

```
vpdn enable
```

```
no vpdn enable
```

Syntax Description	
	This command has no arguments or keywords.

## vpdn group

To associate a virtual private dialup network (VPDN) group to a customer or VPDN profile, use the **vpdn group** customer profile or VPDN profile configuration command. To remove the VPDN group from a customer profile or VPDN profile, use the **no** form of this command.

**vpdn group** *name*

**no vpdn group** *name*

---

### Syntax Description

<i>name</i>	Name of the VPDN group.
-------------	-------------------------

---

## vpdn history failure table-size

To set the failure history table depth, use the **vpdn history failure table-size** global configuration command.

**vpdn history failure table-size** *entries*

---

### Syntax Description

<i>entries</i>	Number of entries. Valid entries are 20 to 50.
----------------	--

---

## vpdn incoming

The **vpdn incoming** command is replaced by the **accept dialin** command. See the description of the **accept dialin** command for more information.

## vpdn logging

To enable the logging of virtual private dialup network (VPDN) events, use the **vpdn logging** global configuration command. To disable the logging of VPDN events, use the **no** form of this command.

**vpdn logging** [**local** | **remote**]

**no vpdn logging** [**local** | **remote**]

---

### Syntax Description

<b>local</b>	(Optional) Logs VPDN events locally.
<b>remote</b>	(Optional) Logs VPDN events to a remote tunnel endpoint.

---

## vpdn logging history failure

To enable the logging of failure events to the failure history table, use the **vpdn logging history failure** global configuration command. To disable the logging of failure events, use the **no** form of this command.

**vpdn logging history failure**

**no vpdn logging history failure**

---

**Syntax Description** This command has no arguments or keywords.

## vpdn outgoing

The **vpdn outgoing** command is replaced by the **request dialin** command. See the description of the **request dialin** command for more information.

## vpdn profile

To combine session counting over virtual private dialup network (VPDN) groups, use the **vpdn profile** customer profile configuration command. To remove a VPDN profile from a customer profile, use the **no** form of this command.

**vpdn profile** *name*

**no vpdn profile** *name*

---

**Syntax Description** *name* VPDN profile name.

---

## vpdn search-order

To specify how the service provider network access server is to perform virtual private dialup network (VPDN) tunnel authorization searches, use the **vpdn search-order** global configuration command. To remove a prior specification, use the **no** form of this command.

**vpdn search-order** { **dnis domain** | **domain dnis** | **domain** | **dnis** }

**no vpdn search-order**

---

<b>Syntax Description</b>	<b>dnis domain</b>	Searches first on the Dialed Number Information Service (DNIS) information provided on ISDN lines and then searches on the domain name.
	<b>domain dnis</b>	Searches first on the domain name and then searches on the DNIS information.
	<b>domain</b>	Searches on the domain name only.
	<b>dnis</b>	Searches on the DNIS information only.

---

## vpdn session-limit

To limit the number of simultaneous VPN sessions that can be established on a router, use the **vpdn session-limit** global configuration command. To allow an unlimited number of simultaneous VPN sessions, use the **no** form of this command.

**vpdn session-limit** *sessions*

**no vpdn session-limit**

---

<b>Syntax Description</b>	<i>sessions</i>	Maximum number of simultaneous VPN sessions that are allowed on a router.
---------------------------	-----------------	---

---

## vpdn softshut

To prevent new sessions from being established on a VPN tunnel without disturbing existing sessions, use the **vpdn softshut** global configuration command. To return the VPN tunnel to active service, use the **no** form of this command.

**vpdn softshut**

**no vpdn softshut**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

## vpdn source-ip

To set the source IP address of the network access server, use the **vpdn source-ip** global configuration command. To disable this function, use the **no** form of this command.

**vpdn source-ip** *ip-address*

**no vpdn source-ip** *ip-address*

---

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the network access server.
---------------------------	-------------------	--

---

## vty-async

To configure all virtual terminal lines on a router to support asynchronous protocol features, use the **vty-async** global configuration command. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

**vty-async**

**no vty-async**

---

**Syntax Description** This command has no arguments or keywords.

## vty-async dynamic-routing

To enable dynamic routing on all virtual asynchronous interfaces, use the **vty-async dynamic-routing** global configuration command. To disable asynchronous protocol features on virtual terminal lines, and therefore disable routing on virtual terminal lines, use the **no** form of this command.

**vty-async dynamic-routing**

**no vty-async dynamic-routing**

---

**Syntax Description** This command has no arguments or keywords.

## vty-async header-compression

To compress the headers of all TCP packets on virtual asynchronous interfaces, use the **vty-async header-compression** global configuration command. To disable virtual asynchronous interfaces and header compression, use the **no** form of this command.

**vty-async header-compression [passive]**

**no vty-async header-compression**

---

<b>Syntax Description</b>	<b>passive</b> (Optional) Outgoing packets are compressed only when TCP incoming packets on the same virtual asynchronous interface are compressed. For SLIP, if you do not specify this option, the Cisco IOS software will compress all traffic. The default is no compression. For PPP, the Cisco IOS software always negotiates header compression.
---------------------------	---

---

## vty-async ipx ppp-client loopback

To enable IPX-PPP on virtual terminal lines, use the **vty-async ipx ppp-client loopback** global configuration command. To disable IPX-PPP sessions on virtual terminal lines, use the **no** form of this command.

**vty-async ipx ppp-client loopback** *number*

**no vty-async ipx ppp-client loopback**

---

### Syntax Description

<i>number</i>	Number of the loopback interface configured for IPX to which the virtual terminal lines are assigned.
---------------	---

---

## vty-async keepalive

To change the frequency of keepalive packets on all virtual asynchronous interfaces, use the **vty-async keepalive** global configuration command. To disable asynchronous protocol features on virtual terminal lines, use the **no vty-async keepalive** command. To disable keepalive packets on virtual terminal lines, use the **vty-async keepalive 0** command.

**vty-async keepalive** *seconds*

**no vty-async keepalive**

**vty-async keepalive 0**

---

### Syntax Description

<i>seconds</i>	Frequency, in seconds, with which the Cisco IOS software sends keepalive messages to the other end of a virtual asynchronous interface. To disable keepalive packets, use a value of 0. The active keepalive interval range is 1 to 32,767 seconds. The default is 10 seconds.
----------------	--

---

## vty-async mtu

To set the maximum transmission unit (MTU) size on virtual asynchronous interfaces, use the **vty-async mtu** global configuration command. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

**vty-async mtu** *bytes*

**no vty-async**

---

### Syntax Description

<i>bytes</i>	MTU size of IP packets that the virtual asynchronous interface can support. The default MTU is 1500 bytes, the minimum MTU is 64 bytes, and the maximum is 1,000,000 bytes.
--------------	---

---

## vty-async ppp authentication

To enable PPP authentication on virtual asynchronous interfaces, use the **vty-async ppp authentication** global configuration command. To disable PPP authentication, use the **no** form of this command.

```
vty-async ppp authentication { chap | pap }
```

```
no vty-async ppp authentication { chap | pap }
```

---

### Syntax Description

<b>chap</b>	Enables CHAP on all virtual asynchronous interfaces.
<b>pap</b>	Enables PAP on all virtual asynchronous interfaces.

---

## vty-async ppp use-tacacs

To enable TACACS authentication for PPP on virtual asynchronous interfaces, use the **vty-async ppp use-tacacs** global configuration command. To disable TACACS authentication on virtual asynchronous interfaces, use the **no** form of this command.

```
vty-async ppp use-tacacs
```

```
no vty-async ppp use-tacacs
```

---

### Syntax Description

This command has no arguments or keywords.

## vty-async virtual-template

To configure virtual terminal lines to support asynchronous protocol functions based on the definition of a virtual interface template, use the **vty-async virtual-template** global configuration command. To disable virtual interface templates for asynchronous functions on virtual terminal lines, use the **no** form of this command.

```
vty-async virtual-template number
```

```
no vty-async virtual-template
```

---

### Syntax Description

<i>number</i>	Virtual interface number.
---------------	---------------------------

---

## x25 aodi

To enable the Always On/Dynamic ISDN (AO/DI) client on an interface, use the **x25 aodi** interface configuration command. To remove AO/DI client functionality, use the **no** form of this command.

**x25 aodi**

**no x25 aodi**

**Syntax Description** This command has no arguments or keywords.

## x25 map ppp

To enable a PPP session over the X.25 protocol, use the **x25 map ppp** interface configuration command. To remove a prior mapping, use the **no** form of this command.

**x25 map ppp** *x121-address* **interface** *cloning-interface* [**no-outgoing**]

**no x25 map ppp** *x121-address* **interface** *cloning-interface* [**no-outgoing**]

<b>Syntax Description</b>	<i>x121-address</i>	X.121 address as follows: <ul style="list-style-type: none"> <li>• Client side—The calling number.</li> <li>• Server side—The called number.</li> </ul>
	<b>interface</b> <i>cloning-interface</i>	Interface to be used for cloning the configuration.
	<b>no-outgoing</b>	(Optional) Ensures that the X.25 map does not originate calls.





## **Terminal Services**





## Terminal Services Commands: **absolute-timeout** Through **show xremote line**

This chapter describes the function and syntax of the terminal services commands: **absolute-timeout** through **show xremote line**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Terminal Services Command Reference*.

### **absolute-timeout**

To set the interval for closing the connection, use the **absolute-timeout** line configuration command. To restore the default, use the **no** form of this command.

**absolute-timeout** *minutes*

**no absolute-timeout**

---

**Syntax Description**

---

<i>minutes</i>	Number of minutes after which the user session will be terminated.
----------------	--

---

### **access-class (LAT)**

To define restrictions on incoming and outgoing connections, use the **access-class** line configuration command. To remove the access list number, use the **no** form of this command.

**access-class** *access-list-number* {**in** | **out**}

**no access-class** *access-list-number*

---

**Syntax Description**

---

<i>access-list-number</i>	Specifies an integer from 1 to 199 that defines the access list.
<b>in</b>	Controls which nodes can make local-area transport (LAT) connections into the server.
<b>out</b>	Defines the access checks made on outgoing connections. (A user who types a node name at the system prompt to initiate a LAT connection is making an outgoing connection.)

---

## arap dedicated

To configure a line to be used only as an AppleTalk Remote Access (ARA) connection, use the **arap dedicated** line configuration command. To return the line to interactive mode, use the **no** form of this command.

**arap dedicated**

**no arap dedicated**

---

**Syntax Description** This command has no arguments or keywords.

## arap enable

To enable AppleTalk Remote Access (ARA) for a line, use the **arap enable** line configuration command. To disable ARA, use the **no** form of this command.

**arap enable**

**no arap enable**

---

**Syntax Description** This command has no arguments or keywords.

## arap net-access-list

To control Apple Macintosh access to networks, use the **arap net-access-list** line configuration command. To return to the default setting, use the **no** form of this command.

**arap net-access-list** *net-access-list-number*

**no arap net-access-list** *net-access-list-number*

---

**Syntax Description** *net-access-list-number* One of the *list* values configured using the AppleTalk **access-list cable-range**, **access-list includes**, **access-list network**, **access-list other-access**, or **access-list within** command.

---

## arap network

To create a new network or zone and cause it to be advertised, use the **arap network** global configuration command. To prevent a new network or zone from being advertised, use the **no** form of this command.

**arap network** [*network-number*] [*zone-name*]

**no arap network**

<b>Syntax Description</b>	<i>network-number</i>	(Optional) AppleTalk network number. The network number must be unique on your AppleTalk network. This network is where all AppleTalk Remote Access (ARAP) users appear when they dial in to the network.
	<i>zone-name</i>	(Optional) AppleTalk zone name.

## arap noguest

To prevent Apple Macintosh guests from logging in to the router, use the **arap noguest** line configuration command. To remove this restriction, use the **no** form of this command.

**arap noguest** [*if-needed*]

**no arap noguest**

<b>Syntax Description</b>	<i>if-needed</i>	(Optional) Does not authenticate if the user already provided authentication. This allows users to log in as guests if they have already been authenticated through a username or password.
---------------------------	------------------	---

## arap require-manual-password

To require users to enter their password manually at the time they log in, use the **arap require-manual-password** line configuration command. To disable the manual password-entry requirement, use the **no** form of this command.

**arap require-manual-password**

**no arap require-manual-password**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## arap timelimit

To set the maximum length of an AppleTalk Remote Access (ARA) session for a line, use the **arap timelimit** line configuration command. To return to the default of unlimited session length, use the **no** form of this command.

**arap timelimit** [*minutes*]

**no arap timelimit**

---

### Syntax Description

*minutes* (Optional) Maximum length of time, in minutes, for a session.

---

## arap warningtime

To set when a disconnect warning message is displayed, use the **arap warningtime** line configuration command. To disable this function, use the **no** form of this command.

**arap warningtime** [*minutes*]

**no arap warningtime**

---

### Syntax Description

*minutes* (Optional) Amount of time, in minutes, before the configured session time limit. At the configured amount of time before a session is to be disconnected, the router sends a message to the Apple Macintosh client, which causes a warning message to appear on the user screen.

---

## arap zonelist

To control which zones the Apple Macintosh client sees, use the **arap zonelist** line configuration command. To disable the default setting, use the **no** form of this command.

**arap zonelist** *zone-access-list-number*

**no arap zonelist** *zone-access-list-number*

---

### Syntax Description

*zone-access-list-number* One of the *list* values configured using the AppleTalk **access-list zone** or **access-list additional-zones** command.

---

## async default ip address

The **async default ip address** command is replaced by the **peer default ip address** command. See the description of the **peer default ip address** command for more information.

## autocommand

To automatically execute a command when a user connects to a particular line, use the **autocommand** line configuration command. To disable the automatic execution, use the **no** form of this command.

**autocommand** *command*

**no autocommand** *command*

<b>Syntax Description</b>	<i>command</i>	Any appropriate EXEC command, including the host name and any switches that occur with the EXEC command.
---------------------------	----------------	--

## busy-message

To create a “host failed” message that displays when a connection fails, use the **busy-message** global configuration command. To disable the “host failed” message from displaying on the specified host, use the **no** form of this command.

**busy-message** *host-name d message d*

**no busy-message** *host-name*

<b>Syntax Description</b>	<i>host-name</i>	Name of the host that cannot be reached.
	<i>d</i>	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.
	<i>message</i>	Message text.

## clear entry

To delete an entry from the list of queued host-initiated connections, use the **clear entry** EXEC command at the system prompt.

**clear entry** *number*

<b>Syntax Description</b>	<i>number</i>	An entry number obtained from the <b>show entry</b> EXEC command.
---------------------------	---------------	---

# connect

To log in to a host that supports Telnet, rlogin, or local-area transport (LAT), use the **connect EXEC** command.

```
connect host [port] [keyword]
```

## Syntax Description

<i>host</i>	A host name or an IP address.
<i>port</i>	(Optional) A decimal TCP port number; the default is the Telnet router port (decimal 23) on the host.
<i>keyword</i>	(Optional) One of the keywords listed in Table 49.

**Table 49 connect Keyword Options**

Option	Description
<b>/debug</b>	Enables Telnet debugging mode.
<b>/encrypt kerberos</b>	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem.  If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
<b>/line</b>	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the Enter key. You can edit the line using the standard Cisco IOS software command editing characters. The <b>/line</b> keyword is a local switch; the remote router is not notified of the mode change.
<b>/noecho</b>	Disables local echo.
<b>/quiet</b>	Prevents onscreen display of all messages from the Cisco IOS software.
<b>/route path</b>	Specifies loose source routing. The <i>path</i> argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
<b>/source-interface</b>	Specifies the source interface.
<b>/stream</b>	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
<b>port-number</b>	Port number.
<b>bgp</b>	Border Gateway Protocol.
<b>chargen</b>	Character generator.
<b>cmd rcmd</b>	Remote commands.
<b>daytime</b>	Daytime.
<b>discard</b>	Discard.
<b>domain</b>	Domain Naming Service.

**Table 49** *connect Keyword Options (continued)*

<b>Option</b>	<b>Description</b>
<b>echo</b>	Echo.
<b>exec</b>	EXEC.
<b>finger</b>	Finger.
<b>ftp</b>	File Transfer Protocol.
<b>ftp-data</b>	FTP data connections (used infrequently).
<b>gopher</b>	Gopher.
<b>hostname</b>	Host name server.
<b>ident</b>	Ident Protocol.
<b>irc</b>	Internet Relay Chat.
<b>klogin</b>	Kerberos login.
<b>kshell</b>	Kerberos shell.
<b>login</b>	Login (rlogin).
<b>lpd</b>	Printer service.
<b>nntp</b>	Network News Transport Protocol.
<b>node</b>	Connect to a specific LAT node.
<b>pop2</b>	Post Office Protocol v2.
<b>pop3</b>	Post Office Protocol v3.
<b>port</b>	Destination LAT port name.
<b>smtp</b>	Simple Mail Transport Protocol.
<b>sunrpc</b>	Sun Remote Procedure Call.
<b>syslog</b>	Syslog.
<b>tacacs</b>	Specify TACACS security.
<b>talk</b>	Talk.
<b>telnet</b>	Telnet.
<b>time</b>	Time.
<b>uucp</b>	UNIX-to-UNIX Copy Program.
<b>whois</b>	Nickname.
<b>www</b>	World Wide Web.

## ip alias

To assign an IP address to the service provided on a TCP port, use the **ip alias** interface configuration command. To remove the specified address for the router, use the **no** form of this command.

```
ip alias ip-address tcp-port
```

```
no ip alias ip-address
```

Syntax	Description
<i>ip-address</i>	Specifies the IP address for the service.
<i>tcp-port</i>	Specifies the number of the TCP port.

## ip local pool

To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, use the **ip local pool** global configuration command. To remove a range of addresses from a pool (longer form of the **no** command), or to delete an address pool (shorter form of the **no** command), use the **no** form of this command.

```
ip local pool { default | pool-name low-ip-address [high-ip-address] }
```

```
no ip local pool { default | pool-name low-ip-address [high-ip-address] }
```

```
no ip local pool { default | pool-name }
```

Syntax	Description
<b>default</b>	Defaults local address pool that is used if no other pool is named.
<i>pool-name</i>	Name of a specific local address pool.
<i>low-ip-address</i>	Lowest IP address in the pool.
<i>high-ip-address</i>	(Optional) Highest IP address in the pool. If this value is omitted, only the <i>low-ip-address</i> IP address argument is included in the local pool.

## ipx nasi-server enable

To enable NetWare Access Server Interface (NASI) clients to connect to asynchronous devices attached to your router, use the **ipx nasi-server enable** global configuration command. To prevent NASI clients from connecting through a router, use the **no** form of this command.

```
ipx nasi-server enable
```

```
no ipx nasi-server enable
```

Syntax	Description
<b>ipx nasi-server enable</b>	This command has no arguments or keywords.

## keymap

To define specific characteristics of keyboard mappings, use the **keymap** global configuration command. To remove the named keymap from the current image of the configuration file, use the **no** form of this command.

**keymap** *keymap-name* *keymap-entry*

**no keymap** *keymap-name*

<b>Syntax Description</b>	<i>keymap-name</i> Name of the file containing the keyboard mappings. The name can be up to 32 characters long and must be unique.
	<i>keymap-entry</i> Commands that define the keymap.

## keymap-type

To specify the keyboard map for a terminal connected to the line, use the **keymap-type** line configuration command. To reset the keyboard type for the line to the default, use the **no** form of this command.

**keymap-type** *keymap-name*

**no keymap-type**

<b>Syntax Description</b>	<i>keymap-name</i> Name of a keymap defined within the configuration file of the router. The TN3270 terminal-type negotiations use the specified keymap type when setting up a connection with the remote host.
---------------------------	---

## lat

To connect to a local-area transport (LAT) host, use the **lat** EXEC command.

**lat** *name* [**node** *nodename* | **port** *portname* | **/debug**]

<b>Syntax Description</b>	<i>name</i> LAT-learned service name.
	<b>node</b> <i>nodename</i> (Optional) Specifies a connection to a particular LAT node that offers a service. If you do not include the node name option, the node with the highest rating offering the service is used. Use the <b>show lat nodes</b> EXEC command to display information about all known LAT nodes.

<b>port</b> <i>portname</i>	(Optional) Specifies a destination LAT port name. This keyword is ignored in most time-sharing systems, but is used by routers and network access servers offering <i>reverse LAT</i> services. Reverse LAT involves connecting to one router from another, so that the target router runs the host portion of the protocol. Enter the port name in the format of the remote system as the <i>portname</i> argument.
<b>/debug</b>	(Optional) Enables a switch to display parameter changes and other special messages.

## lat access-list

To specify access conditions to nodes on the local-area transport (LAT) network, use the **lat access-list** global configuration command. To remove a specified access list number, use the **no** form of this command.

**lat access-list** *number* {**permit** | **deny**} *nodename*

**no lat access-list** *number*

### Syntax Description

<i>number</i>	Specifies a number from 1 to 199 assigned to the line using the <b>access-class</b> line configuration command.
<b>permit</b>	Allows any matching node name to access the line.
<b>deny</b>	Denies access to any matching node name.
<i>nodename</i>	Specifies the name of the LAT node, with or without regular expression pattern matching characters, with which to compare for access. The UNIX-style regular expression characters allow for pattern matching of characters and character strings in the node name.

## lat enabled

To enable local-area transport (LAT), use the **lat enabled** interface configuration command. To disable LAT, use the **no** form of this command.

**lat enabled**

**no lat enabled**

### Syntax Description

This command has no arguments or keywords.

## lat group-list

To allow a name to be assigned to the group list, use the **lat group-list** global configuration command. To remove the specified group list, use the **no** form of this command.

**lat group-list** *groupname* {*number* | *range* | **all**} [**enabled** | **disabled**]

**no lat group-list** *groupname* {*number* | *range* | **all**} [**enabled** | **disabled**]

Syntax Description		
	<i>groupname</i>	Specifies a group code name.
	<i>number</i>	Specifies a group code number. You can enter both a group code name and group code numbers.
	<i>range</i>	Specifies a hyphenated range of numbers.
	<b>all</b>	Specifies the range from 0 to 255.
	<b>enabled</b>	(Optional) Allows incremental changes to the list; that is, you can add a group code without retyping the entire command.
	<b>disabled</b>	(Optional) Allows selective removal of a group code from the list.

## lat host-buffers

To set the number of receive buffers that will be negotiated when the router is acting as a local-area transport (LAT) host, use the **lat host-buffers** global configuration command. To return to the default of one receive buffer, use the **no** form of this command.

**lat host-buffers** *receive-buffers*

**no lat host-buffers** *receive-buffers*

Syntax Description		
	<i>receive-buffers</i>	Integer from 1 to 128 that specifies the number of receive buffers that will be negotiated.

## lat ka-timer

To set the rate of the keepalive timer, use the **lat ka-timer** global configuration command. To restore the default, use the **no** form of this command.

**lat ka-timer** *seconds*

**no lat ka-timer**

Syntax Description		
	<i>seconds</i>	Timer rate, in seconds.

## lat node

To change the local-area transport (LAT) node name without changing the system host name, use the **lat node** global configuration command.

```
lat node node-name
```

Syntax Description	
<i>node-name</i>	Name of the LAT node.

## lat out-group

To define a group list for outgoing user-initiated connections on a line, use the **lat out-group** line configuration command. To return to the default value, use the **lat out-group 0** command.

```
lat out-group {groupname number | range | all}
```

Syntax Description	
<i>groupname</i>	Group code name.
<i>number</i>	Group code number. You can also enter both a group code name and group code numbers.
<i>range</i>	Hyphenated range of numbers.
<b>all</b>	Range from 0 to 255.

## lat remote-modification

To enable remote local-area transport (LAT) modification of line characteristics (for example, baud rate), use the **lat remote-modification** line configuration command. To disable remote LAT modification of line characteristics, use the **no** form of this command.

```
lat remote-modification
```

```
no lat remote-modification
```

Syntax Description	
	This command has no arguments or keywords.

## lat retransmit-limit

To set the number of times that local-area transport (LAT) resends a message before declaring the remote system unreachable, use the **lat retransmit-limit** global configuration command. To restore the default retry value, use the **no** form of this command.

**lat retransmit-limit** *number*

**no lat retransmit-limit**

---

**Syntax Description**

*number*                      Number of retries; any number from 4 to 255.

---

## lat server-buffers

To set the number of receive buffers that will be negotiated when the router is acting as a local-area transport (LAT) server, use the **lat server-buffers** global configuration command. To return to the default of one receive buffer, use the **no** form of this command.

**lat server-buffers** *receive-buffers*

**no lat server-buffers** *receive-buffers*

---

**Syntax Description**

*receive-buffers*            Integer from 1 to 128 that specifies the number of receive buffers that will be negotiated.

---

## lat service-announcements

To reenab le local-area transport (LAT) broadcast service announcements, use the **lat service-announcements** global configuration command. To disable the sending of LAT service announcements, use the **no** form of this command.

**lat service-announcements**

**no lat service-announcements**

---

**Syntax Description**

This command has no arguments or keywords.

## lat service enabled

To enable inbound connections to the specified service and enable the advertisement of this service to routers on the network, use the **lat service enabled** global configuration command. To delete the named service, use the **no** form of this command.

**lat service** *service-name* **enabled**

**no lat service** *service-name* **enabled**

---

### Syntax Description

*service-name* Name of the service.

---

## lat service-group

To specify a group code mask to use when advertising all services for this node and to control incoming services, use the **lat service-group** global configuration command. To remove the group code mask specified, use the **no** form of this command.

**lat service-group** {*groupname* | *number* | *range* | **all**} [**enabled** | **disabled**]

**no lat service-group** {*groupname* | *number* | *range* | **all**} [**enabled** | **disabled**]

---

### Syntax Description

*groupname* Specifies a group code name.

*number* Specifies a group code number.

*range* Specifies a hyphenated range of numbers from 0 to 255.

**all** Specifies the range from 0 to 255.

**enabled** (Optional) Allows incremental changes to the list; that is, you can add a group code without retyping the entire command.

**disabled** (Optional) Allows selective removal of a group code from the list.

---

## lat service ident

To set the local-area transport (LAT) service identification for a specified service, use the **lat service ident** global configuration command. To remove the identification, use the **no** form of this command.

**lat service** *service-name* **ident** *identification*

**no lat service** *service-name* **ident**

---

### Syntax Description

*service-name* Name of the service.

*identification* Descriptive name (text only) that identifies the service.

---

## lat service password

To set up a local-area transport (LAT) password for a service, use the **lat service password** global configuration command. To remove the password, use the **no** form of this command.

```
lat service service-name password password
```

```
no lat service service-name password
```

---

**Syntax Description**

---

*service-name* Name of the service.

---

*password* Password used to gain access to the service.

---

## lat service rating

To set a static service rating for the specified service, use the **lat service rating** global configuration command. To remove the service rating, use the **no** form of this command.

```
lat service service-name rating static-rating
```

```
no lat service service-name rating
```

---

**Syntax Description**

---

*service-name* Name of the service.

---

*static-rating* Static service rating. The rating must be in the range from 1 to 255.

---

## lat service-responder

To configure a node to act as proxy for other nodes when a solicit-information multicast message is received, use the **lat service-responder** global configuration command. To remove any proxy definition set up using the **lat service-responder** command, use the **no** form of this command.

```
lat service-responder
```

```
no lat service-responder
```

---

**Syntax Description**

This command has no arguments or keywords.

## lat service rotary

To associate a rotary group with a service, use the **lat service rotary** global configuration command. To remove the association, use the **no** form of this command.

```
lat service service-name rotary group-number
```

```
no lat service service-name rotary
```

Syntax Description		
	<i>service-name</i>	Name of the service.
	<i>group-number</i>	Rotary group number.

## lat service-timer

To adjust the time between local-area transport (LAT) service advertisements, use the **lat service-timer** global configuration command. To return to the default setting, use the **no** form of this command.

**lat service-timer** *interval*

**no lat service-timer**

Syntax Description		
	<i>interval</i>	Number of seconds between service announcements. Note that the granularity offered by this command is 10-second intervals, and the <i>interval</i> value is rounded up.

## lat vc-sessions

To set the maximum number of sessions to be multiplexed onto a single local-area transport (LAT) virtual circuit, use the **lat vc-sessions** global configuration command. To remove the definition of a prior session, use the **no** form of this command.

**lat vc-sessions** *maximum-number*

**no lat vc-sessions** *maximum-number*

Syntax Description		
	<i>maximum-number</i>	Specifies the number of sessions that will be multiplexed onto a single LAT virtual circuit. This number cannot be greater than 255.

## lat vc-timer

To set the interval of time local-area transport (LAT) waits before sending any traffic, use the **lat vc-timer** global configuration command. To remove a timer definition, use the **no** form of this command.

**lat vc-timer** *milliseconds*

**no lat vc-timer** *milliseconds*

Syntax Description		
	<i>milliseconds</i>	Timer value. Specifies the amount of time LAT will wait before sending traffic. Acceptable values are from 10 to 1000 milliseconds.

## login (EXEC)

To change a login username, use the **login** EXEC command.

**login**

**Syntax Description** This command has no arguments or keywords.

## login (line)



**Note**

This command cannot be used with AAA/TACACS+. Cisco recommends that you use the **login authentication** command instead of the **login** line configuration command. Refer to the *Cisco IOS Security Command Reference* for a description of the **login authentication** command.

To enable password checking at login, use the **login** line configuration command. To disable password checking and allow connections without a password, use the **no** form of this command.

**login** [local | tacacs]

**no login**

Syntax Description	
<b>local</b>	(Optional) Selects local password checking. Authentication is based on the username specified with the <b>username</b> global configuration command.
<b>tacacs</b>	(Optional) Selects the TACACS-style user ID and password-checking mechanism.

## login-string

To define a string of characters that is sent to a host after a successful Telnet connection, use the **login-string** global configuration command. To remove the login string, use the **no** form of this command.

**login-string** *host-name d message [%secp] [%secw] [%b] [%m] d*

**no login-string** *host-name*

Syntax Description	
<i>host-name</i>	Specifies the name of the host.
<i>d</i>	Sets a delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the busy message.
<i>message</i>	Specifies the login string.
<i>%secp</i>	(Optional) Sets a pause in seconds. To insert pauses into the login string, embed a percent sign (%) followed by the number of seconds to pause and the letter “p.”

<i>%secw</i>	(Optional) Prevents users from issuing commands or keystrokes during a pause.
<i>%b</i>	(Optional) Sends a Break character.
<i>%m</i>	(Optional) Supports TN3270 terminals. Sends only CR and no LINE FEED.

## pad

To log in to a packet assembler/disassembler (PAD), use the **pad** EXEC command.

```
pad {x121-address | host-name} [/ cud text] [/ debug] [/ profile name] [/ quiet message] [/ reverse]
[/ use-map]
```

### Syntax Description

<i>x121-address</i>	Specifies the X.121 address of the X.25 host.
<i>host-name</i>	Specifies the X.25 host name if the host-to-address mapping has been set with the <b>X.25 host</b> command.
<b>/ cud</b> <i>text</i>	(Optional) Includes the specified <i>text</i> in the Call User Data (CUD) field of the outgoing Call Request Packet.
<b>/ debug</b>	(Optional) Displays the informational level of logging messages whenever the remote host changes an X.3 parameter setting or sends any other X.29 control packet.
<b>/ profile</b> <i>name</i>	(Optional) Sets X.3 PAD parameters for the <i>name</i> script. Using this keyword and profile name argument is the same as issuing the <b>x29 profile</b> global configuration command when translating X.25. If the X.29 profile is set to <b>default</b> , the profile is applied to all incoming X.25 PAD calls, including the calls used for protocol translation.
<b>/ quiet</b> <i>message</i>	(Optional) Suppresses information messages. Replace the <i>message</i> argument with the actual message that you want to suppress.
<b>/ reverse</b>	(Optional) Causes reverse-charge calls to be accepted on a per-call (rather than a per-interface) basis.
<b>/ use-map</b>	(Optional) Applies <b>x25 map pad</b> command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing PAD call. This function occurs only if a matching X.121 destination address exists in an <b>x25 map pad</b> command entry.

## peer default ip address

To specify an IP address, an address from a specific IP address pool, or an address from the Dynamic Host Configuration Protocol (DHCP) mechanism to be returned to a remote peer connecting to this interface, use the **peer default ip address** interface configuration command. To disable a prior peer IP address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

```
peer default ip address {ip-address |  dhcp |  pool [pool-name]}
```

```
no peer default ip address
```

Syntax Description	
<i>ip-address</i>	Specific IP address to be assigned to a remote peer dialing in to the interface. To prevent duplicate IP addresses from being assigned on more than one interface, this argument cannot be applied to a dialer rotary group nor to an ISDN interface.
<b>dhcp</b>	Retrieves an IP address from the DHCP server.
<b>pool</b>	Uses the global default mechanism as defined by the <b>ip address-pool</b> command unless the optional <i>pool-name</i> argument is supplied. This is the default.
<i>pool-name</i>	(Optional) Name of a local address pool created using the <b>ip local pool</b> command. Retrieve an address from this pool regardless of the global default mechanism setting.

## resume (setting X.3 PAD parameters)

To set X.3 parameters, use the **resume EXEC** command.

```
resume [connection] [/set parameter:value]
```

Syntax Description	
<i>connection</i>	(Optional) The name or number of the connection; the default is the most recent connection.
<i>/set parameter:value</i>	(Optional) Sets the X.3 connection options and packet assembler/disassembler (PAD) parameters for the Cisco IOS software. See Table 50 for the PAD parameter numbers  Refer to the chapter “Configuring the Cisco PAD Facility for X.25 Connections” of the <i>Cisco IOS Terminal Services Configuration Guide</i> for a list of these connection options.

**Table 50 PAD Parameters**

Parameter	Action	Value	Description
1	Escape from data transfer	—	Not supported.
2	Local echo mode	0	No local echo (incoming PAD connection default).
		1	Local echo on (outgoing connection default).
3	Data forward character	0	None—full packet.
		1	Forward packet on receipt of an alphanumeric character.
		2	Forward packet on receipt of a RETURN (outgoing connection default).
		4	Forward packet on receipt of ESCAPE, BEL, ENQ, or ACK.
		8	Forward packet on receipt of DEL, CAN, or DC2.
		16	Forward packet on receipt of ETX or EOT.
		32	Forward packet on receipt of HT, LT, VT, or FF.
64	All other characters in the ASCII chart.		

Table 50 PAD Parameters (continued)

Parameter	Action	Value	Description
4	Idle timer	0	No timer.
		1–255	Delay value in twentieths of a second (default for both connection types is 1).
5	Device control	—	Sends flow control characters during data transfer to the terminal, which controls the terminal and data flow.
6	PAD service signals	—	Not supported.
7	Receipt of break	0	Ignore the Break signal.
		1	Send an INTERRUPT packet to notify the remote host or another PAD that the Break signal was generated.
		2	Send a RESET packet to reset the virtual circuit.
		4	Send an X.29 break indication to the remote host, or to a PAD (outgoing connection default).
		8	Escape from data transfer mode.
		16	Discard output to the terminal by setting parameter 8 to a value of 1.
8	Discard output	0	Normal data delivery to the terminal (outgoing connection default).
		1	Discard all output to the terminal; set by parameter 7.
9	Return padding	—	Determines if PAD can provide padding (insert filler characters) upon receipt of a Return character from the terminal.
10	Line folding	—	Not supported.

Table 50 PAD Parameters (continued)

Parameter	Action	Value	Description
11	Baud rate	10	50 baud.
		5	75 baud.
		9	100 baud.
		0	110 baud.
		1	134.5 baud.
		6	150 baud.
		8	200 baud.
		2	300 baud.
		4	600 <sup>1</sup> baud.
		3	1200 baud.
		7	1800 baud.
		11	75/1200 <sup>2</sup> baud.
		12	2400 baud.
		13	4800 baud.
		14	9600 baud.
15	19200 baud.		
16	48000 baud.		
17	56000 baud.		
18	64000 baud.		
12	Input flow control	—	Determines whether the terminal can send ASCII XON/XOFF (transmission on and off) characters to PAD during the data transfer mode.
13	Line feed insertion	0	Do not insert (outgoing connection default).
		1	Insert after sending RETURN to the terminal.
		2	Insert after echoing RETURN to the terminal.
		4	Insert after echoing RETURN to the remote host.
14	Line feed padding	—	Determines if PAD can provide padding (insert filler characters) upon receipt of a LINE FEED character from the terminal.
15	Local editing	0	Disable editing capabilities.
		1	Enable editing capabilities.
16	Character delete	0–127	Select one ASCII character. Default is ASCII 127 (Del).
17	Line delete	0–127	Select one ASCII character. Default is ASCII 21 (Ctrl-U).
18	Line display	0–127	Select one ASCII character. Default is ASCII 18 (Ctrl-R).
19	Editing PAD service signals	—	Not supported.
20	Echo mask	—	Not supported.

**Table 50** PAD Parameters (continued)

Parameter	Action	Value	Description
21	Parity treatment	—	Not supported.
22	Page wait	—	Not supported.

1. 600 is the beginning of values that are PAD-type dependent.
2. 75 is from PAD; 1200 is to PAD.

## resume (switching sessions)

To switch to another open Telnet, rlogin, local-area transport (LAT), or packet assembler/disassembler (PAD) session, use the **resume** EXEC command.

```
resume [connection] [keyword] [/set parameter:value]
```

### Syntax Description

<i>connection</i>	(Optional) The name or number of the connection; the default is the most recent connection.
<i>keyword</i>	(Optional) One of the options listed in Table 51.
<i>/set parameter:value</i>	(Optional) Sets PAD parameters for the Cisco IOS software (see Table 50).

**Table 51** Telnet and rlogin resume Options

Option	Description
<b>/debug</b>	Displays parameter changes and messages. In the Cisco IOS software, this option displays informational messages whenever the remote host changes an X.3 parameter, or sends an X.29 control packet.
<b>/echo</b>	Performs local echo.
<b>/line</b>	Enables line-mode editing.
<b>/nodebug</b>	Cancels printing of parameter changes and messages.
<b>/noecho</b>	Disables local echo.
<b>/noline<sup>1</sup></b>	Disables line mode and enables character-at-a-time mode, which is the default.
<b>/nostream</b>	Disables stream processing.
<i>/set parameter:value</i>	Sets X.3 connection options. Refer to the chapter “Configuring the Cisco PAD Facility for X.25 Connections” of the <i>Cisco IOS Terminal Services Configuration Guide</i> for a list of these connection options.
<b>/stream</b>	Enables stream processing.

1. **/noline** is the default keyword.

# rlogin

To log in to a UNIX host using rlogin, use the **rlogin** EXEC command.

```
rlogin host [-I username] [/user username] [/quiet] [debug]
```

Syntax Description		
	<i>host</i>	Specifies the host name or IP address.
	<b>-I</b> <i>username</i>	(Optional) The Berkeley Standard Distribution (BSD) UNIX syntax that specifies a username for the remote login. If you do not use this option, the remote username is your local username.
	<b>/user</b> <i>username</i>	(Optional) The EXEC command syntax that specifies a remote username in the initial exchange with the remote host. The rlogin protocol will not present you with the <code>login</code> prompt.
	<b>/quiet</b>	(Optional) Prevents onscreen display of all messages from the Cisco IOS software.
	<b>debug</b>	(Optional) Enables debugging output from the rlogin protocol.

## rlogin trusted-localuser-source

To choose an authentication method for determining the local username to send to the remote rlogin server, use the **rlogin trusted-localuser-source** global configuration command. To restore the default rlogin behavior, use the **no** form of this command.

```
rlogin trusted-localuser-source [local | radius | tacacs]
```

```
no rlogin trusted-localuser-source [local | radius | tacacs]
```

Syntax Description		
	<b>local</b>	(Optional) Uses local username from any authentication method.
	<b>radius</b>	(Optional) Uses local username from RADIUS authentication.
	<b>tacacs</b>	(Optional) Uses local username from TACACS authentication.

## rlogin trusted-remoteuser-source local

To determine the remote username to send to the remote rlogin server, use the **rlogin trusted-remoteuser-source local** global configuration command. To restore the default rlogin behavior, which is to prompt the user for the remote username, use the **no** form of this command.

```
rlogin trusted-remoteuser-source local
```

```
no rlogin trusted-remoteuser-source local
```

Syntax Description	
	This command has no arguments or keywords.

## rxspeed

To set the terminal receive speed (how fast the terminal receives information from the modem), use the **rxspeed** line configuration command. To reset the default value, use the **no** form of this command.

```
rxspeed bps
```

```
no rxspeed bps
```

---

<b>Syntax Description</b>	<i>bps</i>	Baud rate in bits per second (bps).
---------------------------	------------	-------------------------------------

---

## service exec-callback

To enable call back to clients who request a callback from the EXEC level, use the **service exec-callback** global configuration command.

```
service exec-callback
```

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## service old-slip-prompts

To provide backward compatibility for client software scripts expecting Serial Line Internet Protocol (SLIP) and PPP dialogs to be formatted with Cisco IOS software Release 9.1 or earlier releases, use the **service old-slip-prompts** global configuration command. To disable this function, use the **no** form of this command.

```
service old-slip-prompts
```

```
no service old-slip-prompts
```

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## service pt-vty-logging

To log the X.121 calling address, Call User Data (CUD), and IP address assigned to a vty asynchronous connection, use the **service pt-vty-logging** global configuration command. To disable this function, use the **no** form of this command.

```
service pt-vty-logging
```

```
no service pt-vty-logging
```

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## session-limit

To set the maximum number of terminal sessions per line, use the **session-limit** line configuration command. To remove any specified session limit, use the **no** form of this command.

**session-limit** *session-number*

**no session-limit**

<b>Syntax Description</b>	<i>session-number</i>	Specifies the maximum number of sessions.
---------------------------	-----------------------	---

## session-timeout

To set the interval for closing the connection when there is no input or output traffic, use the **session-timeout** line configuration command. To remove the timeout definition, use the **no** form of this command.

**session-timeout** *minutes* [**output**]

**no session-timeout**

<b>Syntax Description</b>	<i>minutes</i>	Specifies the timeout interval in minutes.
	<b>output</b>	(Optional) Specifies that when traffic is sent to an asynchronous line from the router (within the specified interval), the connection is retained.

## show arap

To display information about a running AppleTalk Remote Access Protocol (ARAP) connection, use the **show arap** EXEC command.

**show arap** [*line-number*]

<b>Syntax Description</b>	<i>line-number</i>	(Optional) Number of the line on which an ARAP connection is established and active.
---------------------------	--------------------	--

## show entry

To display the list of queued host-initiated connections to a router, use the **show entry** EXEC command.

**show entry**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## show keymap

To test for the availability of a keymap after a connection on a router takes place, use the **show keymap EXEC** command.

```
show keymap [keymap-name | all]
```

---

### Syntax Description

*keymap-name* (Optional) Name of the keymap.

**all** (Optional) Lists the names of all defined keymaps. The name of the default keymap is not listed.

---

## show lat advertised

To display the local-area transport (LAT) services a router offers to other systems running LAT on the network, use the **show lat advertised EXEC** command.

```
show lat advertised
```

---

### Syntax Description

This command has no arguments or keywords.

## show lat groups

To display the groups that were defined in the Cisco IOS software with the **lat group-list** command, use the **show lat groups EXEC** command.

```
show lat groups
```

---

### Syntax Description

This command has no arguments or keywords.

## show lat nodes

To display information about all known local-area network (LAT) nodes, use the **show lat nodes EXEC** command.

```
show lat nodes
```

---

### Syntax Description

This command has no arguments or keywords.

## show lat services

To display information about learned local-area transport (LAT) services in the Cisco IOS software, use the **show lat services** EXEC command.

```
show lat services [service-name]
```

---

<b>Syntax Description</b>	<i>service-name</i> (Optional) Name of a specific LAT service.
---------------------------	--

---

## show lat sessions

To display active local-area transport (LAT) sessions, use the **show lat sessions** EXEC command.

```
show lat sessions [line-number]
```

---

<b>Syntax Description</b>	<i>line-number</i> (Optional) Displays an active LAT session on a specific line.
---------------------------	--

---

## show lat traffic

To display information about traffic and resource utilization statistics on all active lines, use the **show lat traffic** EXEC command.

```
show lat traffic
```

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

## show line

To display parameters of a terminal line, use the **show line** EXEC command.

```
show line [line-number]
```

---

<b>Syntax Description</b>	<i>line-number</i> (Optional) Absolute line number of the line for which you want to list parameters.
---------------------------	---

---

## show node

To display information about local-area transport (LAT) nodes, use the **show node** EXEC command.

```
show node [all | node-name] [counters | status | summary]
```

Syntax Description		
	<b>all</b>	(Optional) Specifies all nodes.
	<i>node-name</i>	(Optional) Indicates the name of the node for which status is required.
	<b>counters</b>	(Optional) Specifies the various node counters.
	<b>status</b>	(Optional) Specifies detailed node status. This is the default if a node name is specified.
	<b>summary</b>	(Optional) Specifies a status summary for the node. This is the default if no node name is specified.

## show service

To display specific local-area transport (LAT) learned services, use the **show service** EXEC command.

```
show service [service-name]
```

Syntax Description	
	<i>service-name</i> (Optional) The name of a specific LAT service.

## show terminal

To obtain information about the terminal configuration parameter settings for the current terminal line, use the **show terminal** EXEC command.

```
show terminal
```

Syntax Description	
	This command has no arguments or keywords.

## show tn3270 ascii-hexval

To determine ASCII-hexadecimal character mappings, use the **show tn3270 ascii-hexval** EXEC command.

```
show tn3270 ascii-hexval
```

Syntax Description	
	This command has no arguments or keywords.

## show tn3270 character-map

To display character mappings between ASCII and EBCDIC, use the **show tn3270 character-map EXEC** command.

```
show tn3270 character-map {all | ebcdic-in-hex}
```

Syntax Description	all	Displays all nonstandard character mappings.
	<i>ebcdic-in-hex</i>	Displays the ASCII mapping for a specific EBCDIC character.

## show translate

To view translation sessions that have been configured, use the **show translate** privileged EXEC command.

```
show translate
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

## show ttycap

To test for the availability of a ttycap after a connection on a router takes place, use the **show ttycap EXEC** command.

```
show ttycap [ttycap-name | all]
```

Syntax Description	<i>ttycap-name</i>	(Optional) Name of a ttycap.
	<b>all</b>	(Optional) Lists the names of all defined ttycaps. The name of the default ttycap is not listed.

## show users

To display information about the active lines on the router, use the **show users EXEC** command.

```
show users [all]
```

Syntax Description	all	(Optional) Specifies that all lines be displayed, regardless of whether anyone is using them.
--------------------	-----	---

## show x25 pad

To display information about current open connections, including packet transmissions, X.3 parameter settings, and the current status of virtual circuits, use the **show x25 pad** EXEC command.

**show x25 pad**

---

**Syntax Description** This command has no arguments or keywords.

## show xremote

To display XRemote connections and monitor XRemote traffic through the router, use the **show xremote** EXEC command.

**show xremote**

---

**Syntax Description** This command has no arguments or keywords.

## show xremote line

To list XRemote connections and monitor XRemote traffic, use the **show xremote line** EXEC command.

**show xremote line** *number*

---

<b>Syntax Description</b>	<i>number</i>	A decimal value representing the number of virtual terminal lines about which to display information.
---------------------------	---------------	---

---



## Terminal Services Commands: **slip** Through **xremote xdm**

---

This chapter describes the function and syntax of the terminal services commands: **slip** through **xremote xdm**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Terminal Services Command Reference*.

### **slip**

To start a serial connection to a remote host by using Serial Line Internet Protocol (SLIP), use the **slip EXEC** command.

```
slip [/default] {remote-ip-address | remote-name} [@tacacs-server] [/routing] [/compressed]
```

---

#### **Syntax Description**

<b>/default</b>	(Optional) Makes a SLIP connection when a default address has been configured.
<i>remote-ip-address</i>	IP address of the client workstation or PC.
<i>remote-name</i>	Name of the client workstation or PC.
<i>@tacacs-server</i>	(Optional) IP address or IP host name of the TACACS server to which your TACACS authentication request is sent.
<b>/routing</b>	(Optional) Indicates that the remote system is a router. Line must be configured for asynchronous routing using SLIP encapsulation.
<b>/compressed</b>	(Optional) Indicates that IP header compression should be negotiated.

# telnet

To log in to a host that supports Telnet, use the **telnet** EXEC command.

```
telnet host [port] [keyword]
```

Syntax Description	host	Description
	<i>host</i>	A host name or an IP address.
	<i>port</i>	(Optional) A decimal TCP port number; the default is the Telnet router port (decimal 23) on the host.
	<i>keyword</i>	(Optional) One of the keywords listed in Table 52.

**Table 52** telnet Keyword Options

Option	Description
<b>/debug</b>	Enables Telnet debugging mode.
<b>/encrypt kerberos</b>	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem.  If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
<b>/line</b>	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the Enter key. You can edit the line using the standard Cisco IOS software command-editing characters. The <b>/line</b> keyword is a local switch; the remote router is not notified of the mode change.
<b>/noecho</b>	Disables local echo.
<b>/quiet</b>	Prevents onscreen display of all messages from the Cisco IOS software.
<b>/route path</b>	Specifies loose source routing. The <i>path</i> argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
<b>/source-interface</b>	Specifies the source interface.
<b>/stream</b>	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
<i>port-number</i>	Port number.
<b>bgp</b>	Border Gateway Protocol.
<b>chargen</b>	Character generator.
<b>cmd rcmd</b>	Remote commands.
<b>daytime</b>	Daytime.
<b>discard</b>	Discard.
<b>domain</b>	Domain Name Service.
<b>echo</b>	Echo.

**Table 52** *telnet Keyword Options (continued)*

Option	Description
<b>exec</b>	EXEC.
<b>finger</b>	Finger.
<b>ftp</b>	File Transfer Protocol.
<b>ftp-data</b>	FTP data connections (used infrequently).
<b>gopher</b>	Gopher.
<b>hostname</b>	Host name server.
<b>ident</b>	Ident Protocol.
<b>irc</b>	Internet Relay Chat.
<b>klogin</b>	Kerberos login.
<b>kshell</b>	Kerberos shell.
<b>login</b>	Login (rlogin).
<b>lpd</b>	Printer service.
<b>nntp</b>	Network News Transport Protocol.
<b>node</b>	Connect to a specific LAT node
<b>pop2</b>	Post Office Protocol v2.
<b>pop3</b>	Post Office Protocol v3.
<b>port</b>	Destination LAT port name.
<b>smtp</b>	Simple Mail Transport Protocol.
<b>sunrpc</b>	Sun Remote Procedure Call.
<b>syslog</b>	Syslog.
<b>tacacs</b>	Specify TACACS security.
<b>talk</b>	Talk.
<b>telnet</b>	Telnet.
<b>time</b>	Time.
<b>uucp</b>	UNIX-to-UNIX Copy Program.
<b>whois</b>	Nickname.
<b>www</b>	World Wide Web.

## telnet break-on-ip

To cause the system to generate a hardware BREAK signal on the EIA/TIA-232 line that is associated with a reverse Telnet connection when a Telnet Interrupt-Process command is received on that connection, use the **telnet break-on-ip** line configuration command.

### **telnet break-on-ip**

#### **Syntax Description**

This command has no arguments or keywords.

## telnet refuse-negotiations

To set a line using Telnet to refuse to negotiate full-duplex, remote echo requests on incoming connections, use the **telnet refuse-negotiations** line configuration command. To disable this function, use the **no** form of this command.

**telnet refuse-negotiations**

**no telnet refuse-negotiations**

---

**Syntax Description** This command has no arguments or keywords.

## telnet speed

To allow negotiation of the transmission speed of the line to a connected device, use the **telnet speed** line configuration command. To disable this function, use the **no** form of this command.

**telnet speed** *default-speed maximum-speed*

**no telnet speed**

---

<b>Syntax Description</b>	<i>default-speed</i>	Line speed, in bits per second, that the Cisco IOS software will use if the device on the other end of the connection has not specified a speed.
	<i>maximum-speed</i>	Maximum speed, in bits per second, that the device on the port will use.

---

## telnet sync-on-break

To configure the Cisco IOS software to cause an incoming connection to send a Telnet Synchronize signal when it receives a Telnet BREAK signal, use the **telnet sync-on-break** line configuration command. To disable this function, use the **no** form of this command.

**telnet sync-on-break**

**no telnet sync-on-break**

---

**Syntax Description** This command has no arguments or keywords

## telnet transparent

To configure the Cisco IOS software to send a CARRIAGE RETURN (CR) as a CR followed by a NULL instead of a CR followed by a LINE FEED (LF), use the **telnet transparent** line configuration command. To return to the default setting, use the **no** form of this command.

```
telnet transparent
```

```
no telnet transparent
```

**Syntax Description** This command has no arguments or keywords.

## terminal lat out-group

To temporarily define the list of services to which you or another user can connect, use the **terminal lat out-group EXEC** command.

```
terminal lat out-group group-number [start-end] {disabled | enabled}
```

<b>Syntax Description</b>	<i>group-number</i>	Number of the group that has access to the system through the specified line. This number is identified by the system administrator. You also can specify a range of group numbers. Separate the beginning and end of the range with a hyphen.
	[ <i>start-end</i> ]	(Optional) You can specify a range of group numbers for the <i>group-number</i> argument. Separate the beginning and end of the range with a hyphen.
	<b>disabled</b>	Incrementally removes specified groups from a list.
	<b>enabled</b>	Incrementally adds specified groups to a list.

## terminal lat remote-modification

To set a line running local-area transport (LAT) to be remotely modifiable, use the **terminal lat remote-modification EXEC** command.

```
terminal lat remote-modification
```

**Syntax Description** This command has no arguments or keywords.

## terminal transport preferred

To specify the preferred protocol to use for the current session when a command does not specify one, use the **terminal transport preferred EXEC** command.

```
terminal transport preferred {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}
```

Syntax Description		
<b>all</b>		Specifies all recognized protocols.
<b>lat</b>		Specifies the local-area transport (LAT) protocol.
<b>mop</b>		Specifies the Maintenance Operation Protocol (MOP).
<b>nasi</b>		Specifies the NetWare Asynchronous Services Interface (NASI) protocol.
<b>none</b>		Prevents any protocol selection on the line. The router default is that any unrecognized command is a host name. If the preferred protocol is set to none, the router will not attempt any connections if the command is not recognized.
<b>pad</b>		Specifies X.3 packet assembler/disassembler (PAD), which is used most often to connect a server product to X.25 hosts.
<b>rlogin</b>		Specifies UNIX rlogin.
<b>telnet</b>		Specifies the TCP/IP Telnet protocol.
<b>v120</b>		Selects the V.120 protocol for incoming asynchronous connections over ISDN .

## tn3270

To begin a TN3270 session, use the **tn3270 EXEC** command.

```
tn3270 host
```

Syntax Description	<i>host</i>	
		Name or IP address of a specific host on a network that can be reached by the router. The default terminal emulation mode allows access using a VT100 emulation.

## tn3270 8bit display

To configure the Cisco IOS software to use the mask set by the **data-character-bits {7 | 8}** line configuration command or the **terminal data-character bits {7 | 8} EXEC** command, use the **tn3270 8bit display** line configuration command. To restore the default 7-bit mask used for TN3270 connections, use the **no** form of this command.

```
tn3270 8bit display
```

```
no tn3270 8bit display
```

Syntax Description	
	This command has no arguments or keywords.

## tn3270 8bit transparent-mode

To configure the Cisco IOS software to use the mask set by the **data-character-bits {7 | 8}** line configuration command or the **terminal data-character bits {7 | 8}** EXEC command, use the **tn3270 8bit transparent-mode** line configuration command. To restore the default 7-bit mask used for TN3270 connections, use the **no** form of this command.

```
tn3270 8bit transparent-mode
```

```
no tn3270 8bit transparent-mode
```

---

**Syntax Description** This command has no arguments or keywords.

## tn3270 character-map

To convert incoming EBCDIC characters into ASCII characters, use the **tn3270 character-map** global configuration command. To restore default character mappings, use the **no** form of this command.

```
tn3270 character-map ebcdic-in-hex ascii-in-hex
```

```
no tn3270 character-map {all | ebcdic-in-hex} [ascii-in-hex]
```

---

<b>Syntax Description</b>	<i>ebcdic-in-hex</i>	Hexadecimal value of an EBCDIC character.
	<i>ascii-in-hex</i>	Hexadecimal value of an ASCII character.
	<b>all</b>	Indicates all character mappings.

---

## tn3270 datastream

To enable the TN3270 extended datastream, use the **tn3270 datastream** global configuration command. To return to the normal TN3270 datastream, use the **no** form of this command.

```
tn3270 datastream {extended | normal}
```

```
no tn3270 datastream
```

---

<b>Syntax Description</b>	<b>extended</b>	Extended datastream.
	<b>normal</b>	Normal datastream.

---

## tn3270 null-processing

To specify how NULL signals are handled, use the **tn3270 null-processing** global configuration command. To return to 7171 NULL processing, use the **no** form of this command.

**tn3270 null-processing [3270 | 7171]**

**no tn3270 null-processing [3270 | 7171]**

Syntax Description		
	<b>3270</b>	(Optional) NULLs are compressed out of the string, as on a 3278-x terminal.
	<b>7171</b>	(Optional) NULLs are converted to spaces, as on a 7171 controller.

## tn3270 optimize-cursor-move

To increase performance between a remote user and a TN3270 host by limiting cursor movement information that is sent to user terminals, use the **tn3270 optimize-cursor-move** global configuration command. To ensure that all cursor movement information is sent between the terminal and the TN3270 host, use the **no** form of this command.

**tn3270 optimize-cursor-move**

**no tn3270 optimize-cursor-move**

Syntax Description	
	This command has no arguments or keywords.

## tn3270 reset-required

To lock a terminal after input error until the user resets the terminal, use the **tn3270 reset-required** global configuration command. To return to the default of no reset required, use the **no** form of this command.

**tn3270 reset-required**

**no tn3270 reset-required**

Syntax Description	
	This command has no arguments or keywords.

## tn3270 status-message

To reenable the display of status messages after they have been disabled, use the **tn3270 status-message** global configuration command. To save bandwidth on asynchronous lines by not displaying status messages, use the **no** form of this command.

**tn3270 status-message**

**no tn3270 status-message**

---

**Syntax Description** This command has no arguments or keywords.

## tn3270 typeahead

To buffer keyboard data when a 3278 server is in locked mode, use the **tn3270 typeahead** global configuration command. To disable the typeahead function, use the **no** form of this command.

**tn3270 typeahead**

**no tn3270 typeahead**

---

**Syntax Description** This command has no arguments or keywords.

## translate lat

When receiving a local-area transport (LAT) connection request to a service name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate lat** global configuration command.

**translate lat** *incoming-service-name* [*in-options*] *protocol* *outgoing-address* [*out-options*]  
[*global-options*]

---

<b>Syntax Description</b>	<i>incoming-service-name</i>	A LAT service name. When used on the incoming portion, <i>service-name</i> is the name of the service that users specify when trying to make a translated connection. This name can match the name of final destination resource, but is not required to. This argument is useful when making remote translated connections.
	<i>in-options</i>	(Optional) Incoming connection request option. The <b>unadvertised</b> keyword prevents service advertisements from being broadcast to the network. This option can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)

---

---

*protocol outgoing-address*

A protocol name followed by an IP address or host name. The host name is translated to an IP address during configuration, unless you use the tcp **host-name** option, which allows load balancing by dynamically resolving an IP address from a host name. These arguments can have the following values:

- **x25** *x.121-address*—X.25 and an X.121 address. The X.121 address must conform to specifications provided in the *CCITT 1984 Red Book*. This number generally consists of a portion that is administered by the PDN and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits will be interpreted as a subaddress. The PDN still will route these calls to the interface, and the Cisco IOS software itself will be responsible for dealing with the extra digits appropriately.
- **tcp** *ip-address*—TCP/IP Telnet and a standard IP address or host name. The *ip-address* argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS) or explicit specification in an **ip host** command.
- **slip** *ip-address*—The *ip-address* argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the DNS.
- **ppp** *ip-address*—The *ip-address* argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the DNS.
- **autocommand**—Enables you to specify a string for an outgoing connection. The string executes upon connection to a host. If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, you need to specify the **autocommand arap** string.

The **autocommand** option is necessary for ARA, because ARA does not use addressing, and **autocommand** permits you to invoke the **arap** string.

If the string following **autocommand** has one or more spaces as part of the string, you must place quotation marks (“ ”) around the string. For example, if you specify **autocommand tn3270 abracadabra**, you must enclose **tn3270 abracadabra** in quotes.

The **autocommand** option applies only to outgoing connections.

You can issue any EXEC command and any switch or host name as an argument to the **autocommand** option.

---

---

<i>out-options</i>	<p>(Optional) Outgoing connection request options. These arguments can have the following values:</p> <hr/> <p>X.25 translation options:</p> <ul style="list-style-type: none"><li>• <b>cud</b> <i>c-u-data</i>—Sends the specified Call User Data (CUD) text (<i>c-u-data</i>) as part of an outgoing call request after the protocol identification bytes.</li><li>• <b>no-reverse</b>—Specifies that outgoing calls are not to use reverse charging, when the interface default is that all outgoing calls are reverse charged.</li><li>• <b>profile</b> <i>profile</i>—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the <b>x29 profile</b> command.</li><li>• <b>reverse</b>—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls. This is an outgoing option only.</li></ul> <hr/> <p>Telnet TCP translation option <b>port</b> <i>number</i>. For incoming connections, number of the port to match. The default is port 23 (any port). For outgoing connections, number of the port to use. The default is port 23 (Telnet).</p> <hr/> <p>SLIP and PPP translation options:</p> <ul style="list-style-type: none"><li>• <b>ip-pool</b>—Obtains an IP address from a DHCP proxy client or a local pool. If the <b>scope-name</b> option is not specified, the address is obtained from a DHCP proxy client. If the <b>scope-name</b> option is specified, the IP address is obtained from the specified local pool.</li><li>• <b>scope-name</b>—Specific local scope name from which to obtain an IP address. This option can specify a range of IP addresses.</li><li>• <b>header-compression</b> [<b>passive</b>]—Implements header compression on IP packets only. The <b>passive</b> option for SLIP connections permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the <b>passive</b> option) permits compression on all traffic.</li><li>• <b>routing</b>—Permits routing updates between connections. This option is required if the destination device is not on a subnet connected to one of the interfaces on the router.</li><li>• <b>mtu</b> <i>bytes</i>—Permits you to change the maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is 64 through 1000000 bytes.</li></ul>
--------------------	--

---

---

More PPP translation options:

- **keepalive** *number-of-seconds*—Permits you to specify the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and are sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **authentication {chap | pap}**—Use CHAP or PAP authentication for PPP on virtual asynchronous interfaces. If you specify both options, order is significant; the system will try to use the first authentication type, then the second.
- **ppp use-tacacs**—Enables TACACS authentication for CHAP or PAP on virtual asynchronous interfaces (for PPP only; TACACS authentication is not supported for SLIP).
- **ipx loopback number**—Permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. The **loopback number** option specifies the loopback interface to be created. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the vty line. The vty line is assigned to the loopback interface.

---

*global-options*

(Optional) One or more of the following translation options can be used by any connection type:

- **access-class number**—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is the number (integer) previously assigned to an access list. The standard access list in the range from 1 to 99.
  - **max-users number**—Limits the number of simultaneous users of the translation to *number* (an integer you specify).
  - **local**—Allows Telnet protocol negotiations to *not* be translated.
  - **rotor**—Specifies a rotary among host name addresses.
  - **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the vty lines with the **login** command.
  - **quiet**—Suppresses printing of user-information messages.
-

## translate lat (virtual access interfaces)

When receiving a local-area transport (LAT) connection request to a service name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate lat** global configuration command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template.

```
translate lat incoming-service-name [unadvertised] virtual-template number [global-options]
```

### Syntax Description

<i>incoming-service-name</i>	A LAT service name. When used on the incoming portion of the <b>translate lat</b> command, <i>service-name</i> is the name of the service that users specify when trying to make a translated connection. This name can match the name of the final destination resource, but this match is not required. Such matches can be useful when making remote translated connections.
<b>unadvertised</b>	(Optional) The only incoming connection request option for LAT. Prevents service advertisements from being broadcast to the network. This keyword can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)
<b>virtual-template</b> <i>number</i>	Applies the virtual interface template specified by the <i>number</i> argument in place of outgoing options.
<i>global-options</i>	(Optional) Translation options that can be used by any connection type and can be one or more of the following: <ul style="list-style-type: none"> <li>• <b>access-class</b> <i>number</i>—Allows the incoming call to be used by source hosts that match the access list parameters. The <i>number</i> argument is the number (integer) previously assigned to an access list. The standard access list in the range from 1 to 99.</li> <li>• <b>max-users</b> <i>number</i>—Limits the number of simultaneous users of the translation to <i>number</i> (an integer you specify).</li> <li>• <b>local</b>—Allows Telnet protocol negotiations to <i>not</i> be translated.</li> <li>• <b>rotor</b>—Specifies a rotary among host name addresses.</li> <li>• <b>login</b>—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the <b>login</b> command.</li> <li>• <b>quiet</b>—Suppresses printing of user-information messages.</li> </ul>

## translate tcp

When receiving a TCP connection request to a particular destination address or host name, the Cisco router can automatically translate the request to another outgoing protocol connection type. To set up this automatic translation, use the **translate tcp** global configuration command.

```
translate tcp incoming-address [in-options] protocol outgoing-address [out-options]
[global-options]
```

---

### Syntax Description

<i>incoming-address</i>	TCP/IP Telnet and a standard IP address or host name. The argument <i>ip-address</i> is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS) or explicit specification in an <b>ip host</b> command.
<i>in-options</i>	<p>(Optional) Incoming connection request options. These arguments can have the following values:</p> <p>Telnet TCP translation options:</p> <ul style="list-style-type: none"> <li>• <b>binary</b>—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the protocol translation software and is set automatically when you enter a <b>translate</b> command in the old format.)</li> <li>• <b>port number</b>—For incoming connections, enter the number of the port to match. The default is port 23 (any port). For outgoing connections, enter the number of the port to use. The default is port 23 (Telnet).</li> <li>• <b>printer</b>—Supports LAT and X.25 printing over a TCP network among multiple sites. This option causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been successfully established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this option will force the global option <b>quiet</b> to be applied to the translation.</li> <li>• <b>stream</b>—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This option might be useful for connections to ports running UUCP or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the <b>stream</b> option prevents some of usual problems associated with using Telnet for printers, such as strange events happening to bare carriage returns or line feeds and echoing of data back to VMS systems.</li> </ul>

---

---

<i>protocol</i>	Name of a protocol followed by a service name, IP address, or host name. The
<i>outgoing-address</i>	host name is translated to an IP address during configuration. These arguments can have the following values: <ul style="list-style-type: none"><li>• <b>lat</b> <i>service-name</i>—LAT and a LAT service name. You must learn the service name, through LAT service advertisements, before you can use the service.</li><li>• <b>x25</b> <i>X.121-address</i>—X.25 and an X.121 address. The X.121 address must conform to specifications provided in the <i>CCITT 1984 Red Book</i>. This number generally consists of a portion that is administered by the PDN and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface.</li><li>• <b>slip</b> <i>ip-address</i>—The <i>ip-address</i> argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS). The <b>slip</b> argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.</li><li>• <b>ppp</b> <i>ip-address</i>—The <i>ip-address</i> argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the DNS. The <b>ppp</b> argument applies only to outgoing connections; PPP is not supported for incoming protocol translation connections.</li><li>• <b>autocommand</b>—Enables you to specify a string for an outgoing connection. The string executes upon connection to a host. If you want to enable ARA on an outgoing connection, you need to specify the <b>autocommand arap</b> string. The <b>autocommand</b> option is necessary for ARA, because ARA does not use addressing, and <b>autocommand</b> permits you to invoke the <b>arap</b> string. If the string following <b>autocommand</b> has one or more spaces as part of the string, you must place quotation marks (“ ”) around the string. For example, if you specify <b>autocommand tn3270 abracadabra</b>, you must enclose <b>tn3270 abracadabra</b> in quotes. The <b>autocommand</b> option applies only to outgoing connections. You can issue any EXEC command and any switch or host name as an argument to the <b>autocommand</b> option.</li></ul>

---

---

<i>out-options</i>	<p>(Optional) Outgoing connection request options. These arguments can have the following values:</p> <p>LAT translation options:</p> <ul style="list-style-type: none"> <li>• <b>node</b> <i>node-name</i>—Connects to the specified node (<i>node-name</i>) that offers a service. By default, the connection is made to the highest-rated node that offers the service.</li> <li>• <b>port</b> <i>port-name</i>—Destination LAT port name (<i>port-name</i>) in the format of the remote system. This parameter is usually ignored in most time-sharing systems, but is used by terminal servers that offer reverse-LAT services.</li> </ul> <p>X.25 translation options:</p> <ul style="list-style-type: none"> <li>• <b>cud</b> <i>c-u-data</i>—Sends the specified Call User Data (CUD) text (<i>c-u-data</i>) as part of an outgoing call request after the protocol identification bytes.</li> <li>• <b>no-reverse</b>—Specifies that outgoing calls are not to use reverse charging, when the interface default is that all outgoing calls are reverse charged.</li> <li>• <b>profile</b> <i>profile</i>—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the <b>x29 profile</b> command.</li> <li>• <b>reverse</b>—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls. This is an outgoing option only.</li> </ul> <p>SLIP and PPP translation options:</p> <ul style="list-style-type: none"> <li>• <b>ip-pool</b>—Obtains an IP address from a DHCP proxy client or a local pool. If the <b>scope-name</b> option is not specified, the address is obtained from a DHCP proxy client. If the <b>scope-name</b> option is specified, the IP address is obtained from the specified local pool.</li> <li>• <b>scope-name</b>—Specific local scope name from which to obtain an IP address. This option can specify a range of IP addresses.</li> <li>• <b>header-compression [passive]</b>—Implements header compression on IP packets only. The <b>passive</b> option for SLIP connections permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the <b>passive</b> option) permits compression on all traffic.</li> <li>• <b>routing</b>—Permits routing updates between connections. This option is required if the destination device is not on a subnet connected to one of the interfaces on the router.</li> <li>• <b>mtu</b> <i>bytes</i>—Permits you to change the maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is 64 through 1000000 bytes.</li> </ul>
--------------------	--

---

---

More PPP translation options:

- **keepalive** *number-of-seconds*—Permits you to specify the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and are sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **authentication** { **chap** | **pap** }—Use CHAP or PAP authentication for PPP on virtual asynchronous interfaces. If you specify both options, order is significant; the system will try to use the first authentication type, then the second.
- **ppp use-tacacs**—Enables TACACS authentication for CHAP or PAP on virtual asynchronous interfaces (for PPP only; TACACS authentication is not supported for SLIP).
- **ipx loopback** *number*—Permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. The **loopback** *number* option specifies the loopback interface to be created. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the vty. The vty is assigned to the loopback interface.

---

*global-options* (Optional) Translation options that can be used by any connection type and can be one or more of the following:

- **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is the number (integer) previously assigned to an access list. The standard access list in the range 1 to 99.
  - **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify).
  - **local**—Allows Telnet protocol negotiations to *not* be translated.
  - **rotor**—Specifies a rotary among host-name addresses.
  - **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command.
  - **quiet**—Suppresses printing of user-information messages.
- 

## translate tcp (virtual access interfaces)

When receiving a TCP connection request to a particular destination address or host name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate tcp** global configuration command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template.

```
translate tcp incoming-address [in-options] virtual-template number [global-options]
```

**Syntax Description**

<i>incoming-address</i>	TCP/IP Telnet and a standard IP address or host name. The <i>ip-address</i> argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS) or explicit specification in an <b>ip host</b> command.
<i>in-options</i>	(Optional) Incoming connection request options. These arguments can have the following values: <ul style="list-style-type: none"> <li>• <b>binary</b>—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the Cisco IOS software and is set automatically when you enter a <b>translate</b> command in the old format.)</li> <li>• <b>port number</b>—For incoming connections, enter the number of the port to match. The default is port 23 (any port). For outgoing connections, enter the number of the port to use. The default is port 23 (Telnet).</li> <li>• <b>printer</b>—Supports LAT and X.25 printing over a TCP network among multiple sites. This option causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been successfully established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this option will force the global <b>quiet</b> option to be applied to the translation.</li> <li>• <b>stream</b>—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This option might be useful for connections to ports running UUCP or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the <b>stream</b> option prevents some of the usual problems associated with using Telnet for printers, such as strange events happening to bare carriage returns or line feeds and echoing of data back to VMS systems.</li> </ul>
<b>virtual-template number</b>	Applies the virtual interface template specified by the <i>number</i> argument in place of outgoing options.
<i>global-options</i>	(Optional) One or more of the following translation options can be used by any connection type: <ul style="list-style-type: none"> <li>• <b>access-class number</b>—Allows the incoming call to be used by source hosts that match the access list parameters. The <i>number argument</i> is an integer value previously assigned to an access list. The standard access list is in the range from 1 to 99.</li> <li>• <b>local</b>—Allows Telnet protocol negotiations to <i>not</i> be translated.</li> <li>• <b>login</b>—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the <b>login</b> command.</li> <li>• <b>max-users number</b>—Maximum number of simultaneous users of the translation.</li> <li>• <b>quiet</b>—Suppresses printing of user-information messages.</li> <li>• <b>rotor</b>—Specifies a rotary among host name addresses.</li> </ul>

## translate x25

When receiving an X.25 connection request to a particular destination address, or to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate x25** global configuration command.

```
translate x25 incoming-address [in-options] protocol outgoing-address [out-options]
[global-options]
```

### Syntax Description

<i>incoming-address</i>	X.25 and an X.121 address. The X.121 address must conform to specifications provided in the <i>CCITT 1984 Red Book</i> . This number generally consists of a portion that is administered by the Public Data Network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software itself is responsible for interpreting the extra digits appropriately. Do not use the same address on the interface and for translation.
<i>in-options</i>	(Optional) Incoming connection request options. These arguments can have the following values: <ul style="list-style-type: none"> <li>• <b>accept-reverse</b>—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. This is an incoming option only.</li> <li>• <b>cu</b> <i>c-u-data</i>—Sends the specified Call User Data (CUD) text (<i>c-u-data</i>) as part of an outgoing call request after the protocol identification bytes.</li> <li>• <b>idle</b> <i>minutes</i>—Specifies the number of minutes the virtual circuit is idle. This option enables the protocol translation function to clear a switched virtual circuit after a set period of inactivity, where <i>minutes</i> is the number of minutes in the period. Calls either originated or terminated are cleared. The maximum value of <i>minutes</i> is 255. The default value of <i>minutes</i> is zero.</li> <li>• <b>printer</b>—Supports LAT and TCP printing over an X.25 network among multiple sites. Provides an “interlock mechanism” between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. The option causes the Cisco IOS software to delay the call confirmation of an incoming X.25 call request until the outgoing protocol connection (to TCP or LAT) has been successfully established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being confirmed and then cleared, which is the default behavior. Note that using this option will force the global <b>quiet</b> option to be applied to the translation.</li> <li>• <b>profile</b> <i>profile</i>—Sets the X.3 PAD parameters as defined in the profile created by the <b>x29 profile</b> command.</li> </ul>

---

*protocol outgoing-address* Name of a protocol followed by a service name, IP address, or host name. The host name is translated to an IP address during configuration, unless you use the TCP **host-name** option, which allows load balancing by dynamically resolving an IP address from a host name. These arguments can have the following values:

- **lat** *service-name*—LAT and a LAT service name. You must learn the service name, through LAT service advertisements, before you can use the service.
- **tcp** *ip-address*—TCP/IP Telnet and a standard IP address or host name. The argument *ip-address* is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS) or explicit specification in an **ip host** command.
- **slip** *ip-address*—The *ip-address* argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the DNS. The **slip** argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.
- **ppp** *ip-address*—The *ip-address* argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the DNS. The **ppp** argument applies only to outgoing connections; PPP is not supported for incoming protocol translation connections.
- **autocommand**—Enables you to specify a string for an outgoing connection. The string executes upon connection to a host. If you want to enable the AppleTalk Remote Access Protocol on an outgoing connection, you need to specify the **autocommand arap** string.

The **autocommand** option is necessary for ARA, because ARA does not use addressing, and **autocommand** permits you to invoke the **arap** string.

If the string following **autocommand** has one or more spaces as part of the string, you must place quotation marks (“ ”) around the string. For example, if you specify **autocommand tn3270 abracadabra**, you must enclose the **tn3270 abracadabra** string in quotes.

The **autocommand** option applies only to outgoing connections.

You can issue any EXEC command and any switch or host name as an argument to the **autocommand** option.

---

---

*out-options*

(Optional) Outgoing connection request options. These arguments can have the following values:

- **use-map**—Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing protocol translation call. This application occurs when the protocol translation function searches the X.25 map PAD entries and finds a matching X.121 destination address. The X.25 map facilities applied to the outgoing translation can be viewed with the **show translation** command throughout the duration of the translation session.

LAT translation options:

- **node** *node-name*—Connects to the specified node (*node-name*) that offers a service. By default, the connection is made to the highest-rated node that offers the service.
- **port** *port-name*—Destination LAT port name (*port-name*) in the format of the remote system. This parameter is usually ignored in most time sharing systems, but is used by terminal servers that offer reverse-LAT services.

Telnet TCP translation options:

- **port** *number*—For incoming connections, number of the port to match. The default is port 23 (any port). For outgoing connections, number of the port to use. The default is port 23 (Telnet).

SLIP and PPP translation options:

- **ip-pool**—Obtains an IP address from a DHCP proxy client or a local pool. If the **scope-name** option is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** option is specified, the IP address is obtained from the specified local pool.
  - **scope-name**—Specific local scope name from which to obtain an IP address. This option can specify a range of IP addresses.
  - **header-compression** [**passive**]—Implements header compression on IP packets only. The **passive** option for SLIP connections permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** option) permits compression on all traffic.
  - **routing**—Permits routing updates between connections. This option is required if the destination device is not on a subnet connected to one of the interfaces on the router.
  - **mtu** *bytes*—Permits you to change the maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is 64 to 1000000 bytes.
-

---

 PPP translation options:

- **keepalive** *number-of-seconds*—Permits you to specify the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and are sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 to 32767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in the **more system:running-config** or **show translate** command output.
- **authentication {chap | pap}**—Use CHAP or PAP authentication for PPP on virtual asynchronous interfaces. If you specify both options, order is significant; the system will try to use the first authentication type, then the second.
- **ppp use-tacacs**—Enables TACACS authentication for CHAP or PAP on virtual asynchronous interfaces (for PPP only; TACACS authentication is not supported for SLIP).
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.

---

*global-options*

(Optional) Translation options that can be used by any connection type and can be one or more of the following:

- **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The *number* argument is the number (integer) previously assigned to an access list. The standard access list in the range 1 to 99.
  - **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify).
  - **local**—Prevents Telnet protocol negotiations from being translated.
  - **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command.
  - **rotor**—Specifies a rotary among host name addresses.
  - **quiet**—Suppresses printing of user-information messages.
-

- **swap**—Allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD. For X.25-to-TCP translations only.
- **pvc number** {[**interface serial number**] [**packetsize in-size out-size**] [**window size in-size out-size**]}—Specifies that the incoming or outgoing connection is actually a permanent virtual circuit (PVC). Only one session is allowed per PVC, where:

*number*—Specifies the virtual circuit channel number of the incoming connection, which must be less than the virtual circuits assigned to the SVC.

**interface serial number**—Specifies a PVC interface on which to set up the PVC connection.

**packetsize in-size out-size**—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Following are valid packet size values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.

**window size in-size out-size**—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.

## translate x25 (virtual access interfaces)

When receiving an X.25 connection request to a particular destination address, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate x25** global configuration command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate x25** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template.

```
translate x25 incoming-address [in-options] virtual-template number [global-options]
```

**Syntax Description***incoming-address*

X.25 and an X.121 address. The X.121 address must conform to specifications provided in the *CCITT 1984 Red Book*. This number generally consists of a portion that is administered by the PDN and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software is responsible for interpreting the extra digits. Do not use the same address on the interface and for translation.

*in-options*

(Optional) Incoming connection request options. These arguments can have the following values:

- **accept-reverse**—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. This is an incoming option only.
- **cud *c-u-data***—Sends the specified Call User Data (CUD) text (*c-u-data*) as part of an outgoing call request after the protocol identification bytes.
- **printer**—Supports LAT and TCP printing over an X.25 network among multiple sites. Provides an “interlock mechanism” between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. The option causes the protocol translation software to delay the call confirmation of an incoming X.25 call request until the outgoing protocol connection (to TCP or LAT) has been successfully established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being confirmed and then cleared, which is the default behavior. Note that using this option will force the global option **quiet** to be applied to the translation.
- **profile *profile***—Sets the X.3 PAD parameters as defined in the profile created by the **x29 profile** command.
- **pvc *number***—Specifies that the incoming connection (identified by the *number* argument) is actually a permanent virtual circuit (PVC).

<b>virtual-template</b> <i>number</i>	Applies the virtual interface template specified by the <i>number</i> argument in place of outgoing options.
<i>global-options</i>	(Optional) Translation options that can be used by any connection type and can be one or more of the following: <ul style="list-style-type: none"> <li>• <b>access-class</b> <i>number</i>—Allows the incoming call to be used by source hosts that match the access list parameters. The <i>number</i> argument is an integer in the range from 1 to 99 that was previously assigned to an access list.</li> <li>• <b>local</b>—Allows Telnet protocol negotiations to <i>not</i> be translated.</li> <li>• <b>login</b>—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the <b>login</b> command.</li> <li>• <b>max-users</b> <i>number</i>—Limits the number of simultaneous users of the translation to <i>number</i> (an integer you specify).</li> <li>• <b>quiet</b>—Suppresses printing of user-information messages.</li> <li>• <b>rotor</b>—Specifies a rotary among host name addresses.</li> <li>• <b>swap</b>—Allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This option allows incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The <b>swap</b> keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD. For X.25-to-TCP translations only.</li> </ul>

## transport input

To define which protocols to use to connect to a specific line of the router, use the **transport input** line configuration command.

```
transport input {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}
```

Syntax Description	
<b>all</b>	Selects all protocols.
<b>lat</b>	Selects the Digital LAT protocol and specifies both incoming reverse LAT and host-initiated connections.
<b>mop</b>	Selects Maintenance Operation Protocol (MOP).
<b>nasi</b>	Select NetWare Access Servers Interface (NASI) as the input transport protocol.
<b>none</b>	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.
<b>pad</b>	Selects X.3 packet assembler/disassembler (PAD) incoming connections.
<b>rlogin</b>	Selects the UNIX rlogin protocol.
<b>telnet</b>	Specifies all types of incoming TCP/IP connections.
<b>v120</b>	Selects the V.120 protocol for incoming asynchronous connections over ISDN.

## transport output

To determine the protocols that can be used for outgoing connections from a line, use the **transport output** line configuration command.

**transport output** { **all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120** }

Syntax Description		
	<b>all</b>	Selects all protocols.
	<b>lat</b>	Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
	<b>mop</b>	Selects Maintenance Operation Protocol (MOP).
	<b>nasi</b>	Selects NetWare Access Server Interface (NASI) as the output transport protocol.
	<b>none</b>	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to <b>none</b> , the system no longer makes that assumption. No connection will be attempted if the command is not recognized.
	<b>pad</b>	Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.
	<b>rlogin</b>	Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
	<b>telnet</b>	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
	<b>v120</b>	Selects the V.120 protocol for outgoing asynchronous connections over ISDN.

## transport preferred

To specify the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection, use the **transport preferred** line configuration command.

**transport preferred** { **all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120** }

Syntax Description		
	<b>all</b>	Selects all recognized protocols.
	<b>lat</b>	Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
	<b>mop</b>	Selects Maintenance Operation Protocol (MOP).
	<b>nasi</b>	Selects NetWare Access Server Interface (NASI) protocol.
	<b>none</b>	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to <b>none</b> , the system no longer makes that assumption. No connection is attempted if the command is not recognized.
	<b>pad</b>	Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.

<b>rlogin</b>	Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
<b>telnet</b>	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
<b>v120</b>	Selects the asynchronous protocols over ISDN.

## ttycap

To define characteristics of a terminal emulation file, use the **ttycap** global configuration command. To delete any named ttycap entry from the configuration file, the **no** form of this command.

**ttycap** *ttycap-name termcap-entry*

**no ttycap** *ttycap-name*

<b>Syntax Description</b>	<i>ttycap-name</i>	Name of a file. It can be up to 32 characters long and must be unique.
	<i>termcap-entry</i>	Commands that define the ttycap. Consists of two parts.

## txspeed

To set the terminal transmit speed (how fast the terminal sends information to the modem), use the **txspeed** line configuration command. To return to the default setting, use the **no** form of this command.

**txspeed** *bps*

**no txspeed**

<b>Syntax Description</b>	<i>bps</i>	Baud rate, in bits per second (bps).
---------------------------	------------	--------------------------------------

## where

To list the open sessions, use the **where** EXEC command.

**where**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## x25 subaddress

To append either a physical port number or a value specified for a line as a subaddress to the X.121 calling address, use the **x25 subaddress** line configuration command. To disable subaddressing, the **no** form of this command.

**x25 subaddress** {*line* | *number*}

**no x25 subaddress** {*line* | *number*}

### Syntax Description

<b>line</b>	Physical port number for the indicated line to be appended to the X.121 address as the subaddress.
<i>number</i>	Numeric variable assigned to a specific line.

## x28

To enter X.28 mode and access an X.25 network or set X.3 packet assembler/disassembler (PAD) parameters, use the **x28 EXEC** command. To exit X.28 mode, use the **no** form of this command.

**x28** [**escape** *character-string*] [**noescape**] [**nuicud**] [**profile** *file-name*] [**reverse**] [**verbose**]

**no x28** [**escape** *character-string*] [**noescape**] [**nuicud**] [**profile** *file-name*] [**reverse**] [**verbose**]

### Syntax Description

<b>escape</b> <i>character-string</i>	(Optional) Specifies a character string to use to exit X.28 mode and return to EXEC mode. The character string can be any string of alphanumeric characters. The Ctrl key can be used in conjunction with the character string.
<b>noescape</b>	(Optional) Specifies that no escape character string is defined (user cannot return to EXEC mode). On the console line, the <b>noescape</b> option is ignored, and the default escape sequence is used ( <b>exit</b> command).
<b>nuicud</b>	(Optional) Specifies the network user identification (NUI) data to not be placed in the NUI facility of the call request. Instead the data is placed in the Call User Data (CUD) area of the call request packet.
<b>profile</b> <i>file-name</i>	(Optional) Specifies using a user-configured profile of X.3 parameters. A profile is created with the <b>x29 profile</b> EXEC command.
<b>reverse</b>	(Optional) Specifies reverse charges for outgoing calls made from the local router to the destination device.
<b>verbose</b>	(Optional) Displays optional service signals such as the called DTE address, facility block, and CUD.

## x3

To set X.3 packet assembler/disassembler (PAD) parameters, use the **x3** EXEC command.

**x3** *parameter:value*

---

<b>Syntax Description</b>	<i>parameter:value</i> Sets the PAD parameters.
---------------------------	---

---

## xremote

To prepare the router for manual startup and initiate an XRemote connection, use the **xremote** EXEC command. This command begins the instructions that prompt you through the connection.

**xremote**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

## xremote lat

To initiate a DECwindow session over a local-area transport (LAT) connection, use the **xremote lat** EXEC command.

**xremote lat** *service*

---

<b>Syntax Description</b>	<i>service</i> Name of the desired LAT service.
---------------------------	---

---

## xremote tftp buffersize

To change the buffer size used for loading font files, use the **xremote tftp buffersize** global configuration command. To restore the buffer size to the default value, use the **no** form of this command.

**xremote tftp buffersize** *buffersize*

**no xremote tftp buffersize**

---

<b>Syntax Description</b>	<i>buffersize</i> Buffer size in bytes. This is a decimal number in the range from 4096 to 70000 bytes. The default is 70000.
---------------------------	---

---

## xremote tftp host

To add a specific Trivial File Transfer Protocol (TFTP) font server as a source of fonts for the terminal, use the **xremote tftp host** global configuration command. To remove a font server from the list, use the **no** form of this command.

**xremote tftp host** *host-name*

**no xremote tftp host** *host-name*

---

### Syntax Description

*host-name* IP address or name of the host containing fonts.

---

## xremote tftp retries

To specify the number of retries the font loader will attempt before declaring an error condition, use the **xremote tftp retries** global configuration command. To restore the default retries number, use the **no** form of this command.

**xremote tftp retries** *retries*

**no xremote tftp retries**

---

### Syntax Description

*retries* (Optional) Number of retries. Acceptable values are decimal numbers in the range from 1 to 15.

---

## xremote xdm

To activate automatic session startup for an XRemote connection, use the **xremote xdm EXEC** command.

**xremote xdm** [*host-name*]

---

### Syntax Description

*host-name* (Optional) Host computer name or IP address.

---







## **Switching Services**





## Switching Services Commands: **access-list rate-limit** Through **lane fssrp**

---

This chapter describes the function and syntax of the switching services commands: **access-list rate-limit** through **lane fssrp**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Switching Services Command Reference*.

### **access-list rate-limit**

To configure an access list for use with committed access rate (CAR) policies, use the **access-list rate-limit** global configuration command. To remove the access list from the configuration, use the **no** form of this command.

```
access-list rate-limit acl-index {precedence | mac-address | exp | mask mask}
```

```
no access-list rate-limit acl-index {precedence | mac-address | exp | mask mask}
```

---

#### **Syntax Description**

<i>acl-index</i>	Specifies the access list number. Classification options are as follows: <ul style="list-style-type: none"><li>• For IP precedence, use any number from 1 to 99.</li><li>• For MAC address, use any number from 100 to 199.</li><li>• For MPLS experimental field, use any number from 200 to 299.</li></ul>
<i>precedence</i>	Specifies the IP precedence. Valid values are from 0 to 7.
<i>mac-address</i>	Specifies the MAC address.
<i>exp</i>	Specifies the MPLS experimental field. Valid values are from 0 to 7.
<b>mask</b> <i>mask</i>	Specifies the mask. Use this option if you want to assign multiple IP precedences or MPLS experimental field values to the same rate-limit access list.

---

## address-family

To enter the address family submode for configuring routing protocols such as BGP, RIP, and static routing, use the **address-family** command in address family configuration submode. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

### VPN-IPv4 Unicast

**address-family vpnv4** [**unicast**]

**no address-family vpnv4** [**unicast**]

### IPv4 Unicast

**address-family ipv4** [**unicast**]

**no address-family ipv4** [**unicast**]

### IPv4 Unicast with CE router

**address-family ipv4** [**unicast**] **vrf** *vrf-name*

**no address-family ipv4** [**unicast**] **vrf** *vrf-name*

Syntax Description		
	<b>vpnv4</b>	Configures sessions that carry customer VPN-IPv4 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher.
	<b>ipv4</b>	Configures sessions that carry standard IPv4 address prefixes.
	<b>unicast</b>	(Optional) Specifies unicast prefixes.
	<b>vrf</b> <i>vrf-name</i>	Specifies the name of a VPN routing and forwarding instance (VRF) to associate with submode commands.

## append-after

To insert a path entry after a specified index number, use the **append-after** IP explicit path configuration command.

**append-after** *index command*

Syntax Description		
	<i>index</i>	Previous index number. Valid values are from 0 to 65534.
	<i>command</i>	An IP explicit path configuration command that creates a path entry. (Use the <b>next-address</b> command to specify the next IP address in the explicit path.)

## atm-address

To override the control ATM address of an MPC or MPS, use the **atm-address** command in interface configuration mode. To revert to the default address, use the **no** form of this command.

**atm-address** *atm-address*

**no atm-address**

---

<b>Syntax Description</b>	<i>atm-address</i> Control ATM address.
---------------------------	---

---

## bgp default route-target filter

To enable automatic BGP route-target community filtering, use the **bgp default route-target filter** router configuration command. To disable this feature, use the **no** form of this command.

**bgp default route-target filter**

**no bgp default route-target filter**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## bgp scan-time

To configure scanning intervals of BGP routers to decrease import processing time of VPNv4 routing information, use the **bgp scan-time** command in router configuration mode. To disable the scanning interval of a router, use the **no** form of this command.

**bgp scan-time** [**import**] *scanner-interval*

**no bgp scan-time**

---

<b>Syntax Description</b>	<b>import</b> (Optional) Configures import processing of VPNv4 unicast routing information from BGP routers into routing tables.
<i>scanner-interval</i>	Specifies the scanning interval of BGP routing information. Valid values used for selecting the desired scanning interval are from 5 to 60 seconds.

---

## cable bundle

To configure a cable interface to belong to an interface bundle, use the **cable bundle** interface configuration command. To delete a cable interface bundle definition, use the **no** form of this command.

**cable bundle** *n* [**master**]

**no cable bundle** *n* [**master**]

<b>Syntax Description</b>	<i>n</i>	Specifies the bundle identifier. Valid range is from 1 to 255.
	<b>master</b>	(Optional) Defines the specified interface as the master.

## cable helper-address

To specify a destination address for User Datagram Protocol (UDP) broadcast (DHCP) packets, use the **cable helper-address** interface configuration command. To disable this feature, use the **no** form of this command.

**cable helper-address** *ip-address* { **cable-modem** | **host** }

**no cable helper-address** *ip-address* { **cable-modem** | **host** }

<b>Syntax Description</b>	<i>ip-address</i>	The IP address of a DHCP server.  Based on whether you add the <b>host</b> or <b>cable-modem</b> keyword at the end of the <b>cable helper-address</b> command, it is the IP address of the MSOs CNR server or the ISPs DHCP server.
	<b>cable-modem</b>	Specifies that only cable modem UDP broadcasts are forwarded
	<b>host</b>	Specifies that only host UDP broadcasts are forwarded.

## cache

To configure aggregation cache operational parameters, use the **cache** command in aggregation cache configuration mode. To disable the operational parameters, use the **no** form of this command.

**cache** { **entries** *number* | **timeout** [**active** *minutes* | **inactive** *seconds*] }

**no cache** { **entries** *number* | **timeout** [**active** *minutes* | **inactive** *seconds*] }

<b>Syntax Description</b>	<b>entries</b> <i>number</i>	The number of cached entries allowed in the aggregation cache. The number of entries can be 1024 to 524288. The default is 4096.
	<b>timeout</b>	Dissolves the session in the aggregation cache.

<b>active minutes</b>	(Optional) The number of minutes that an active entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
<b>inactive seconds</b>	(Optional) The number of seconds that an inactive entry will stay in the aggregation cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

## class (MPLS)

To configure a defined MPLS CoS map that specifies how classes map to label VCs (LVCs) when combined with a prefix map, use the **class** command in CoS map submode. To disable this option, use the **no** form of this command.

**class** *class* [**available standard premium control**]

**no class** *class* [**available standard premium control**]

Syntax Description	
<i>class</i>	The precedence of identified traffic to classify traffic.
<b>available</b>	(Optional) Means low precedence (In/Out plus lower two bits = 0,4).
<b>standard</b>	(Optional) Means next precedence (In/Out plus lower two bits = 1,5).
<b>premium</b>	(Optional) Means high precedence (In/Out plus lower two bits = 2,6).
<b>control</b>	(Optional) Means highest precedence pair (In/Out plus lower two bits = 3,7). These bits are reserved for control traffic.

## clear adjacency

To clear the Cisco Express Forwarding (CEF) adjacency table, use the **clear adjacency** command in EXEC mode.

**clear adjacency**

**Syntax Description** This command has no arguments or keywords.

## clear atm vc

To release a specified switched virtual circuit (SVC), use the **clear atm vc** command in EXEC mode.

**clear atm vc** *vcd*

Syntax Description	
<i>vcd</i>	Virtual channel descriptor of the channel to be released.

## clear cef linecard

To clear Cisco Express Forwarding (CEF) information from line cards, use the **clear cef linecard** command in EXEC mode.

```
clear cef linecard [slot-number] [adjacency | interface | prefix]
```

Syntax Description		
	<i>slot-number</i>	(Optional) Line card slot number to clear. When you omit this argument, all line card slots are cleared.
	<b>adjacency</b>	(Optional) Clears line card adjacency tables and rebuilds adjacency for the specified line card.
	<b>interface</b>	(Optional) Clears line card interface information and recreates the interface information for the specified line card.
	<b>prefix</b>	(Optional) Clears line card prefix tables and starts rebuilding the FIB table.

## clear ip cef prefix-statistics

To clear Cisco Express Forwarding (CEF) counters by resetting the packet and byte count to zero (0), use the **clear ip cef prefix-statistics** command in EXEC mode.

```
clear ip cef {network [mask] | *} prefix-statistics
```

Syntax Description		
	<i>network</i>	Clears counters for a FIB entry specified by network.
	<i>mask</i>	(Optional) Clears counters for a FIB entry specified by network and mask.
	*	Clears counters for all FIB entries.

## clear ip flow stats

To clear the NetFlow switching statistics, use the **clear ip flow stats** command in EXEC mode.

```
clear ip flow stats
```

Syntax Description	
	This command has no arguments or keywords.

## clear ip mds forwarding

To clear all linecard routes from a MFIB table and resynchronize it with the Router Processor (RP), use the **clear ip mds forwarding** command in EXEC mode.

```
clear ip mds forwarding
```

**Syntax Description** This command has no arguments or keywords.

## clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** command in EXEC mode.

```
clear ip mroute [* | group [source]]
```

<b>Syntax Description</b>	*	Deletes all entries from the IP multicast routing table.
	<i>group</i>	Either of the following: <ul style="list-style-type: none"> <li>Name of the multicast group, as defined in the DNS hosts table or with the <b>ip host</b> command.</li> <li>IP address of the multicast group. This is a multicast IP address in four-part, dotted notation.</li> </ul>
	<i>source</i>	(Optional) If you specify a group name or address, you can also specify a name or address of a multicast source that is sending to the group. A source need not be a member of the group.

## clear ip pim interface count

To clear all line card counts or packet counts, use the **clear ip pim interface count** command in EXEC mode.

```
clear ip pim interface count
```

**Syntax Description** This command has no arguments or keywords.

## clear ip route vrf

To remove routes from the VRF routing table, use the **clear ip route vrf** command in EXEC mode.

```
clear ip route vrf vrf-name [* | network [mask]]
```

**Syntax Description**

<i>vrf-name</i>	Name of the VPN routing and forwarding instance (VRF) for the static route.
*	Deletes all routes for a given VRF.
<i>network</i>	Destination to be removed, in dotted decimal format.
<i>mask</i>	(Optional) Mask for the specified network destination, in dotted decimal format.

## clear lane le-arp

To clear the dynamic LAN Emulation Address Resolution Protocol (LE ARP) table or a single LE ARP entry of the LANE client configured on the specified subinterface or emulated LAN, use the **clear lane le-arp** command in EXEC mode.

**Cisco 7500 Series**

```
clear lane le-arp [interface slot/port [.subinterface-number] | name elan-name] [mac-address mac-address | route-desc segment segment-number bridge bridge-number]
```

**Cisco 4500 and 4700 Routers**

```
clear lane le-arp [interface number [.subinterface-number] | name elan-name] [mac-address mac-address | route-desc segment segment-number bridge bridge-number]
```

**Syntax Description**

<b>interface</b> <i>slot/port</i> [ <i>.subinterface-number</i> ]	(Optional) Interface or subinterface for the LANE client whose LE ARP table or entry is to be cleared for the Cisco 7500 series routers. The space between the <b>interface</b> keyword and the <i>slot</i> argument is optional.
<b>interface</b> <i>number</i> [ <i>.subinterface-number</i> ]	(Optional) Interface or subinterface for the LANE client whose LE ARP table or entry is to be cleared for the Cisco 4500 or 4700 routers. The space between the <b>interface</b> keyword and the <i>number</i> argument is optional.
<b>name</b> <i>elan-name</i>	(Optional) Name of the emulated LAN for the LANE client whose LE ARP table or entry is to be cleared. Maximum length is 32 characters.
<b>mac-address</b> <i>mac-address</i>	(Optional) Keyword and MAC address of the LANE client.
<b>route-desc segment</b> <i>segment-number</i>	(Optional) Keywords and LANE segment number. The segment number ranges from 1 to 4095.
<b>bridge</b> <i>bridge-number</i>	(Optional) Keyword and bridge number that is contained in the route descriptor. The bridge number ranges from 1 to 15.

## clear lane server

To force a LANE server to drop a client and allow the LANE configuration server to assign the client to another emulated LAN, use the **clear lane server** command in EXEC mode.

### Cisco 7500 Series

```
clear lane server { interface slot/port [.subinterface-number] | name elan-name } [mac-address
mac-address | client-atm-address atm-address | lecid lane-client-id | route-desc segment
segment-number bridge bridge-number]
```

### Cisco 4500 and 4700 Routers

```
clear lane server { interface number [.subinterface-number] | name elan-name } [mac-address
mac-address | client-atm-address atm-address | lecid lecid | route-desc segment
segment-number bridge bridge-number]
```

### Syntax Description

<b>interface</b> <i>slot/port</i> [ <i>.subinterface-number</i> ]	Interface or subinterface where the LANE server is configured for the Cisco 7500 series. The space between the <b>interface</b> keyword and the <i>slot</i> argument is optional.
<b>interface</b> <i>number</i> [ <i>.subinterface-number</i> ]	Interface or subinterface where the LANE server is configured for the Cisco 4500 or 4700 routers. The space between the <b>interface</b> keyword and the <i>number</i> argument is optional.
<b>name</b> <i>elan-name</i>	Name of the emulated LAN on which the LANE server is configured. Maximum length is 32 characters.
<b>mac-address</b> <i>mac-address</i>	(Optional) Keyword and MAC address of the LANE client.
<b>client-atm-address</b> <i>atm-address</i>	(Optional) Keyword and ATM address of the LANE client.
<b>lecid</b> <i>lane-client-id</i>	(Optional) Keyword and ID of the LANE client. The LANE client ID is a value from 1 to 4096.
<b>route-desc segment</b> <i>segment-number</i>	(Optional) Keywords and LANE segment number. The segment number ranges from 1 to 4095.
<b>bridge</b> <i>bridge-number</i>	(Optional) Keyword and bridge number that is contained in the route descriptor. The bridge number ranges from 1 to 15.

## clear mpoa client cache

To clear the ingress and egress cache entries of one or all MPCs, use the **clear mpoa client cache** command in EXEC mode.

```
clear mpoa client [name mpc-name] cache [ingress | egress] [ip-address ip-address]
```

**Syntax Description**

<b>name</b> <i>mpc-name</i>	(Optional) Specifies the name of the MPC with the specified name.
<b>ingress</b>	(Optional) Clears ingress cache entries associated with the MPC.
<b>egress</b>	(Optional) Clears egress cache entries associated with the MPC.
<b>ip-address</b> <i>ip-address</i>	(Optional) Clears matching cache entries with the specified IP address.

## clear mpoa server cache

To clear the ingress and egress cache entries, use the **clear mpoa server cache** command in EXEC mode.

```
clear mpoa server [name mps-name] cache [ingress | egress] [ip-address ip-address]
```

**Syntax Description**

<b>name</b> <i>mps-name</i>	(Optional) Specifies the name of the MPS. If this keyword is omitted, this command will apply to all servers.
<b>ingress</b>	(Optional) Clears ingress cache entries associated with a server.
<b>egress</b>	(Optional) Clears egress cache entries associated with a server.
<b>ip-address</b> <i>ip-address</i>	(Optional) Clears matching cache entries with the specified IP address. If this keyword is omitted, this command will clear all entries.

## client-atm-address name

To add a LANE client address entry to the configuration server's configuration database, use the **client-atm-address name** database configuration command. To remove a client address entry from the table, use the **no** form of this command.

```
client-atm-address atm-address-template name elan-name
```

```
no client-atm-address atm-address-template
```

**Syntax Description**

<i>atm-address-template</i>	Template that explicitly specifies an ATM address or a specific part of an ATM address and uses wildcard characters for other parts of the ATM address, making it easy and convenient to specify multiple addresses matching the explicitly specified part.  Wildcard characters can replace any nibble or group of nibbles in the prefix, the end-system identifier (ESI), or the selector fields of the ATM address.
<i>elan-name</i>	Name of the emulated LAN. Maximum length is 32 characters.

## default

To enable a default aggregation cache, use the **default** command in aggregation cache configuration mode.

**default** [**cache** | **enabled** | **export**]

Syntax Description		
	<b>cache</b>	(Optional) Configures NetFlow cache parameters.
	<b>enabled</b>	(Optional) Enables the aggregation cache.
	<b>export</b>	(Optional) Specifies host or port to send flow statistics.

## default-name

To provide an emulated LAN name in the configuration server's database for those client MAC addresses and client ATM addresses that do not have explicit emulated LAN name bindings, use the **default-name** command in database configuration mode. To remove the default name, use the **no** form of this command.

**default-name** *elan-name*

**no default-name**

Syntax Description		
	<i>elan-name</i>	Default emulated LAN name for any LANE client MAC address or LANE client ATM address not explicitly bound to any emulated LAN name. Maximum length is 32 characters.

## enabled

To enable an aggregation cache, use the **enabled** command in aggregation cache configuration mode.

**enabled**

Syntax Description	
	This command has no arguments or keywords.

## encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs (VLANs), use the **encapsulation dot1q** subinterface configuration command.

**encapsulation dot1q** *vlan-id* [**native**]

Syntax Description		
	<i>vlan-id</i>	Virtual LAN identifier. The allowed range is from 1 to 1000.
	<b>native</b>	(Optional) Sets the PVID value of the port to the <i>vlan-id</i> value.

## encapsulation isl

To enable the Inter-Switch Link (ISL), use the **encapsulation isl** command in subinterface configuration mode.

**encapsulation isl** *vlan-identifier*

<b>Syntax Description</b>	<i>vlan-identifier</i>	Virtual LAN (VLAN) identifier. The allowed range is from 1 to 1000.
---------------------------	------------------------	---

## encapsulation sde

To enable IEEE 802.10 encapsulation of traffic on a specified subinterface in virtual LANs (VLANs), use the **encapsulation sde** command in subinterface configuration mode. IEEE 802.10 is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

**encapsulation sde** *said*

<b>Syntax Description</b>	<i>said</i>	Security association identifier. This value is used as the VLAN identifier. The valid range is from 0 to 0xFFFFFFFFE.
---------------------------	-------------	---

## encapsulation tr-isl trbrf-vlan

To enable TRISL, use the **encapsulation tr-isl trbrf-vlan** command in subinterface configuration mode. TRISL is a Cisco proprietary protocol for interconnecting multiple routers and switches and maintaining VLAN information as traffic goes between switches.

**encapsulation tr-isl trbrf-vlan** *vlan-id* **bridge-num** *bridge-number*

<b>Syntax Description</b>	<i>vlan-id</i>	Number identifying the VLAN.
	<b>bridge-num</b> <i>bridge-number</i>	Keyword and specify the identification number of the bridge number on the ISL trunk. Possible values are from 1 to 4095.

## exit

To leave aggregation cache mode, use the **exit** command in aggregation cache configuration mode.

**exit**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## exit-address-family

To exit from the address family configuration submode, use the **exit-address-family** command in address family configuration submode.

**exit-address-family**

**Syntax Description** This command has no arguments or keywords.

## export destination

To enable the exporting of information from NetFlow aggregation caches, use the **export destination** command in aggregation cache configuration mode. To disable the exporting of NetFlow aggregation cache information, use the **no** form of this command.

**export destination** *ip-address port*

**no export destination** *ip-address port*

<b>Syntax Description</b>	<i>ip-address</i>	Destination IP address.
	<i>port</i>	Destination UDP port.

## extended-port

To associate the currently selected extended MPLS ATM (XTagATM) interface with a particular external interface on the remotely controlled ATM switch, use the **extended-port** interface configuration command.

**extended-port** *ctrl-if* { **bpx** *bpx-port-number* | **descriptor** *vsi-descriptor* | **vsi** *vsi-port-number* }

<b>Syntax Description</b>	<i>ctrl-if</i>	Identifies the ATM interface used to control the remote ATM switch. You must configure VSI on this interface using the <b>tag-control-protocol</b> interface configuration command.
	<b>bpx</b> <i>bpx-port-number</i>	Specifies the associated Cisco BPX interface using the native BPX syntax. <i>slot.port</i> [ <i>virtual port</i> ] You can use this form of the command only when the controlled switch is a Cisco BPX switch.
	<b>descriptor</b> <i>vsi-descriptor</i>	Specifies the associated port by its VSI physical descriptor. The <i>vsi-descriptor</i> string must match the corresponding VSI physical descriptor.
	<b>vsi</b> <i>vsi-port-number</i>	Specifies the associated port by its VSI physical descriptor. The <i>vsi-descriptor</i> string must match the corresponding VSI physical descriptor.

## holding-time

To specify the holding time value for the MPS-p7 variable of an MPS, use the **holding-time** command in MPS configuration mode. To revert to the default value, use the **no** form of this command.

**holding-time** *time*

**no holding-time** *time*

<b>Syntax Description</b>	<i>time</i>	Specifies the holding time value in seconds.
---------------------------	-------------	--

## import map

To configure an import route map for a VRF, use the **import map** command in VRF configuration submode.

**import map** *route-map*

<b>Syntax Description</b>	<i>route-map</i>	Specifies the route map to be used as an import route map for the VRF.
---------------------------	------------------	--

## index

To insert or modify a path entry at a specific index, use the **index ip** explicit path subcommand. To disable this feature, use the **no** form of this command.

**index** *index command*

**no index** *index*

<b>Syntax Description</b>	<i>index</i>	Index number at which the path entry will be inserted or modified. Valid values are from 0 to 65534.
	<i>command</i>	An IP explicit path configuration command that creates or modifies a path entry. (Currently you can use only the <b>next-address</b> command.)

## interface atm

To enter interface configuration mode, specify ATM as the interface type, and create a subinterface on that interface type, use the **interface atm** global configuration command.

**interface atm** *interface.subinterface-number* [**mpls** | **tag-switching** | **point-to-point** | **multipoint**]

Syntax Description		
<i>interface</i>		Specifies a (physical) ATM interface (for example, 3/0).
<i>.subinterface-number</i>		Specifies the subinterface number for the ATM interface. On Cisco 7500 series routers, subinterface numbers can range from 0 to 4294967285.
<b>mpls</b>		(Optional) Specifies MPLS as the interface type for which a subinterface is to be created.
<b>tag-switching</b>		(Optional) Specifies tag switching as the interface type for which a subinterface is to be created.
<b>point-to-point</b>		(Optional) Specifies point-to-point as the interface type for which a subinterface is to be created.
<b>multipoint</b>		(Optional) Specifies multipoint as the interface type for which a subinterface is to be created.

## interface fastethernet

To select a particular Fast Ethernet interface for configuration, use the **interface fastethernet** global configuration command.

### Cisco 4500 and 4700 Series Routers

```
interface fastethernet number
```

### Cisco 7200 Series Routers

```
interface fastethernet slot/port
```

### Cisco 7500 Series Routers

```
interface fastethernet slot/port-adapter/port
```

Syntax Description		
<i>number</i>		Port, connector, or interface card number. On Cisco 4500 or 4700 series routers, specifies the Network Interface Module (NIM) or Networking Products Marketplace (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
<i>slot</i>		Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>		Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>		Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

## interface XTagATM

To enter interface configuration mode for the extended MPLS ATM (XTagATM) interface, use the following **interface XTagATM** global configuration command.

```
interface XTagATM if-num
```

Syntax Description	<i>if-num</i>	Specifies the interface number.
--------------------	---------------	---------------------------------

## ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** command in global configuration mode. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

```
ip cache-invalidate-delay [minimum maximum quiet threshold]
```

```
no ip cache-invalidate-delay
```

Syntax Description	<i>minimum</i>	(Optional) Minimum time (in seconds) between invalidation request and actual invalidation. The default is 2 seconds.
	<i>maximum</i>	(Optional) Maximum time (in seconds) between invalidation request and actual invalidation. The default is 5 seconds.
	<i>quiet</i>	(Optional) Length of quiet period (in seconds) before invalidation.
	<i>threshold</i>	(Optional) Maximum number of invalidation requests considered to be quiet.

## ip cef

To enable Cisco Express Forwarding (CEF) on the route processor card, use the **ip cef** command in global configuration mode. To disable CEF, use the **no** form of this command.

```
ip cef [distributed]
```

```
no ip cef [distributed]
```

Syntax Description	<b>distributed</b>	(Optional) Enables distributed CEF (dCEF) operation. Distributes CEF information to line cards. Line cards perform express forwarding.
--------------------	--------------------	--

## ip cef accounting

To enable network accounting of Cisco Express Forwarding (CEF), use the **ip cef accounting** command in global configuration mode. To disable network accounting of CEF, use the **no** form of this command.

**ip cef accounting** [*per-prefix*] [*non-recursive*]

**no ip cef accounting** [*per-prefix*] [*non-recursive*]

Syntax Description		
	<b>per-prefix</b>	(Optional) Enables the collection of the number of packets and bytes express forwarded to a destination (or prefix).
	<b>non-recursive</b>	(Optional) Enables accounting through nonrecursive prefixes. For prefixes with directly connected next hops, enables the collection of the number of packets and bytes express forwarded through a prefix.

## ip cef traffic-statistics

To change the time interval that controls when NHRP will set up or tear down an SVC, use the **ip cef traffic-statistics** command in global configuration mode. To restore the default values, use the **no** form of this command.

**ip cef traffic-statistics** [*load-interval seconds*] [*update-rate seconds*]

**no ip cef traffic-statistics**

Syntax Description		
	<b>load-interval</b> <i>seconds</i>	(Optional) Length of time (in 30-second increments) during which the average <i>trigger-threshold</i> and <i>teardown-threshold</i> are calculated before an SVC setup or teardown action is taken. (These thresholds are configured in the <b>ip nhrp trigger-svc</b> command.) The <b>load-interval</b> range is 30 seconds to 300 seconds, in 30-second increments. The default value is 30 seconds.
	<b>update-rate</b> <i>seconds</i>	(Optional) Frequency with which the port adapter sends the accounting statistics to the Router Processor (RP). When NHRP is used in distributed CEF switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

## ip dhcp relay information option

To enable the system to insert the cable modem MAC address into a DHCP packet received from a cable modem or host and forward the packet to a DHCP server, use the **ip dhcp relay information option** in global configuration mode. To disable MAC address insertion, use the **no** form of this command.

**ip dhcp relay information option**

**no ip dhcp relay information option**

Syntax Description	
	This command has no keywords or arguments.

## ip explicit-path

To enter the command mode for IP explicit paths and create or modify the specified path, use the **ip explicit-path** command in router configuration mode. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. To disable this feature, use the **no** form of this command.

```
ip explicit-path {name word | identifier number} [{enable | disable}]
```

```
no explicit-path {name word | identifier number}
```

### Syntax Description

<b>name</b> <i>word</i>	Name of the explicit path.
<b>identifier</b> <i>number</i>	Number of the explicit path. Valid values are from 1 to 65535.
<b>enable</b>	(Optional) Enables the path.
<b>disable</b>	(Optional) Prevents the path from being used for routing while it is being configured.

## ip flow-aggregation cache

To enable aggregation cache configuration mode, use the **ip flow-aggregation cache** global configuration command. To disable aggregation cache configuration mode, use the **no** form of this command.

```
ip flow-aggregation cache {as | destination-prefix | prefix | protocol-port | source-prefix}
```

```
no ip flow-aggregation cache {as | destination-prefix | prefix | protocol-port | source-prefix}
```

### Syntax Description

<b>as</b>	Configures the autonomous system aggregation cache scheme.
<b>destination-prefix</b>	Configures the destination prefix aggregation cache scheme.
<b>prefix</b>	Configures the prefix aggregation cache scheme.
<b>protocol-port</b>	Configures the protocol port aggregation cache scheme.
<b>source-prefix</b>	Configures the source prefix aggregation cache scheme.

## ip flow-cache entries

To change the number of entries maintained in the NetFlow cache, use the **ip flow-cache entries** command in global configuration mode. To return to the default number of entries, use the **no** form of this command.

```
ip flow-cache entries number
```

```
no ip flow-cache entries
```

### Syntax Description

<i>number</i>	Number of entries to maintain in the NetFlow cache. The valid range is from 1024 to 524288 entries. The default is 65536 (64K).
---------------	---

## ip flow-export

To enable the exporting of information in NetFlow cache entries, use the **ip flow-export** command in global configuration mode. To disable the exporting of information, use the **no** form of this command.

**ip flow-export** *ip-address udp-port* [**version 1** | **version 5** [**origin-as** | **peer-as**]]

**no ip flow-export**

Syntax Description		
	<i>ip-address</i>	IP address of the workstation to which you want to send the NetFlow information.
	<i>udp-port</i>	UDP protocol-specific port number.
	<b>version 1</b>	(Optional) Specifies that the export packet uses the version 1 format. This is the default. The version field occupies the first two bytes of the export record. The number of records stored in the datagram is a variable from 1 to 24 for version 1.
	<b>version 5</b>	(Optional) Specifies that the export packet uses the version 5 format. The number of records stored in the datagram is a variable between 1 and 30 for version 5.
	<b>origin-as</b>	(Optional) Specifies that export statistics include the origin autonomous system (AS) for the source and destination.
	<b>peer-as</b>	(Optional) Specifies that export statistics include the peer AS for the source and destination.

## ip load-sharing

To enable load balancing for Cisco Express Forwarding (CEF), use the **ip load-sharing** command in interface configuration mode. To disable load balancing for CEF, use the **no** form of this command.

**ip load-sharing** [**per-packet**] [**per-destination**]

**no ip cef** [**per-packet**]

Syntax Description		
	<b>per-packet</b>	(Optional) Enables per-packet load balancing on the interface.
	<b>per-destination</b>	(Optional) Enables per-destination load balancing on the interface.

## ip mroute-cache

To configure IP multicast fast switching or multicast distributed switching (MDS), use the **ip mroute-cache** command in interface configuration mode. To disable either of these features, use the **no** form of this command.

**ip mroute-cache [distributed]**

**no ip mroute-cache [distributed]**

---

### Syntax Description

<b>distributed</b>	(Optional) Enables MDS on the interface. In the case of RSP, this keyword is optional; if it is omitted, fast switching occurs. On the GSR, this keyword is required because the GSR does only distributed switching.
--------------------	---

---

## ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

**ip multicast-routing [distributed]**

**no ip multicast-routing**

---

### Syntax Description

<b>distributed</b>	(Optional) Enables MDS.
--------------------	-------------------------

---

## ip route-cache

To control the use of high-speed switching caches for IP routing, use the **ip route-cache** command in interface configuration mode. To disable any of these switching modes, use the **no** form of this command.

**ip route-cache [cbus]**

**no ip route-cache [cbus]**

**ip route-cache same-interface**

**no ip route-cache same-interface**

**ip route-cache [flow]**

**no ip route-cache [flow]**

**ip route-cache distributed**

**no ip route-cache distributed**

<b>Syntax Description</b>	<b>cbus</b>	(Optional) Enables both autonomous switching and fast switching.
	<b>same-interface</b>	Enables fast-switching packets to back out through the interface on which they arrived.
	<b>flow</b>	(Optional) Enables the RSP to perform flow switching on the interface.
	<b>distributed</b>	Enables VIP distributed switching on the interface. This feature can be enabled on Cisco 7500 series routers with an RSP and VIP controllers. If both the <b>ip route-cache flow</b> and <b>ip route-cache distributed</b> commands are configured, the VIP does distributed flow switching. If only the <b>ip route-cache distributed</b> command is configured, the VIP does distributed switching.

## ip route-cache cef

To enable Cisco Express Forwarding (CEF) operation on an interface after CEF operation has been disabled, use the **ip route-cache cef** command in interface configuration mode. To disable CEF operation on an interface, use the **no** form of this command.

**ip route-cache cef**

**no ip route-cache cef**

**Syntax Description** This command has no arguments or keywords.

## ip route-cache flow

To enable NetFlow switching for IP routing, use the **ip route-cache flow** command in interface configuration mode. To disable NetFlow switching, use the **no** form of this command.

**ip route-cache flow**

**no ip route-cache flow**

**Syntax Description** This command has no arguments or keywords.

## ip route vrf

To establish static routes for a VPN routing and forwarding (VRF) instance, use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

**ip route vrf** *vrf-name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]*

**no ip route vrf** *vrf-name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]*

<b>Syntax Description</b>	<i>vrf-name</i>	Name of the VPN routing/forwarding instance (VRF) for the static route.
	<i>prefix</i>	IP route prefix for the destination, in dotted-decimal format.
	<i>mask</i>	Prefix mask for the destination, in dotted-decimal format.
	<i>next-hop-address</i>	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
	<i>interface</i>	(Optional) Type of network interface to use: ATM, Ethernet, loopback, POS (packet over SONET), or null.
	<i>interface-number</i>	(Optional) Number identifying the network interface to use.
	<b>global</b>	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
	<i>distance</i>	(Optional) An administrative distance for this route.
	<b>permanent</b>	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
	<b>tag tag</b>	(Optional) Label (tag) value that can be used for controlling redistribution of routes through route maps.

## ip vrf forwarding

To associate a VPN routing and forwarding (VRF) instance with an interface or subinterface, use the **ip vrf forwarding** command in global configuration mode or interface configuration mode. To disassociate a VRF, use the **no** form of this command.

```
ip vrf forwarding vrf-name
```

```
no ip vrf forwarding vrf-name
```

<b>Syntax Description</b>	<i>vrf-name</i>	Name assigned to a VRF.
---------------------------	-----------------	-------------------------

## ip vrf

To configure a VPN routing and forwarding (VRF) routing table, use the **ip vrf** command in global configuration mode or router configuration mode. To remove a VRF routing table, use the **no** form of this command.

```
ip vrf vrf-name
```

```
no ip vrf vrf-name
```

<b>Syntax Description</b>	<i>vrf-name</i>	Name assigned to a VRF.
---------------------------	-----------------	-------------------------

## keepalive-lifetime

To specify the duration that a keepalive message from an MPS is considered valid by the MPC, use the **keepalive-lifetime** command in global configuration mode.

**keepalive-lifetime** *time*

<b>Syntax Description</b>	<i>time</i>	Time (in seconds) for the MPS-p2 variable of the MPS. The default value is 35 seconds.
---------------------------	-------------	--

## keepalive-time

To specify the keepalive time value for the MPS-p1 variable of an MPS, use the **keepalive-time** command in MPS configuration mode. To revert to the default value, use the **no** form of this command.

**keepalive-time** *time*

**no keepalive-time** *time*

<b>Syntax Description</b>	<i>time</i>	Specifies the keepalive time value (in seconds).
---------------------------	-------------	--

## lane auto-config-atm-address

To specify that the configuration server ATM address is computed by the Cisco automatic method, use the **lane auto-config-atm-address** command in interface configuration mode. To remove the previously assigned ATM address, use the **no** form of this command.

**lane** [**config**] **auto-config-atm-address**

**no lane** [**config**] **auto-config-atm-address**

<b>Syntax Description</b>	<b>config</b>	(Optional) When the <b>config</b> keyword is used, this command applies only to the LAN Emulation Configuration Server (LECS). This keyword indicates that the LECS should use the auto computed LECS address.
---------------------------	---------------	--

## lane bus-atm-address

To specify an ATM address—and thus override the automatic ATM address assignment—for the broadcast and unknown server on the specified subinterface, use the **lane bus-atm-address** command in interface configuration mode. To remove the ATM address previously specified for the broadcast and unknown server on the specified subinterface and thus revert to the automatic address assignment, use the **no** form of this command.

**lane bus-atm-address** *atm-address-template*

**no lane bus-atm-address** [*atm-address-template*]

<b>Syntax Description</b>	<i>atm-address-template</i>	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the end-system identifier (ESI) bytes, or the selector byte of the automatically assigned ATM address.
---------------------------	-----------------------------	---

## lane client

To activate a LANE client on the specified subinterface, use the **lane client** command in interface configuration mode. To remove a previously activated LANE client on the subinterface, use the **no** form of this command.

**lane client** {**ethernet** | **tokenring**} [*elan-name*]

**no lane client** [{**ethernet** | **tokenring**} [*elan-name*]]

<b>Syntax Description</b>	<b>ethernet</b>	Identifies the emulated LAN (ELAN) attached to this subinterface as an Ethernet ELAN.
	<b>tokenring</b>	Identifies the ELAN attached to this subinterface as a Token Ring ELAN.
	<i>elan-name</i>	(Optional) Name of the ELAN. This argument is optional because the client obtains its ELAN name from the configuration server. The maximum length of the name is 32 characters.

## lane client-atm-address

To specify an ATM address—and thus override the automatic ATM address assignment—for the LANE client on the specified subinterface, use the **lane client-atm-address** command in interface configuration mode. To remove the ATM address previously specified for the LANE client on the specified subinterface and thus revert to the automatic address assignment, use the **no** form of this command.

**lane client-atm-address** *atm-address-template*

**no lane client-atm-address** [*atm-address-template*]

---

<b>Syntax Description</b>	<i>atm-address-template</i>	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the ESI bytes, or the selector byte of the automatically assigned ATM address.
---------------------------	-----------------------------	---

---

## lane client flush

To enable the flush mechanism of a LAN Emulation Client (LEC), use the **lane client flush** global configuration command. To disable the flush mechanism of a LEC, use the **no** form of this command.

**lane client flush**

**no lane client flush**

---

<b>Syntax Description</b>	This command contains no arguments or keywords.
---------------------------	---

---

## lane client mpoa client name

To bind a LEC to the named MPC, use the **lane client mpoa client name** command in interface configuration mode. To unbind the named MPC from a LEC, use the **no** form of this command.

**lane client mpoa client name** *mpc-name*

**no lane client mpoa client name** *mpc-name*

---

<b>Syntax Description</b>	<i>mpc-name</i> Name of the specific MPC.
---------------------------	---

---

## lane client mpoa server name

To bind a LEC with the named MPS, use the **lane client mpoa server name** command in interface configuration mode. To unbind the server, use the **no** form of this command.

**lane client mpoa server name** *mps-name*

**no lane client mpoa server name** *mps-name*

---

<b>Syntax Description</b>	<i>mps-name</i> Name of the specific MPOA server.
---------------------------	---

---

## lane config-atm-address

To specify a configuration server's ATM address explicitly, use the **lane config-atm-address** command in interface configuration mode. To remove an assigned ATM address, use the **no** form of this command.

**lane** [**config**] **config-atm-address** *atm-address-template*

**no lane** [**config**] **config-atm-address** *atm-address-template*

<b>Syntax Description</b>	<b>config</b>	(Optional) When the <b>config</b> keyword is used, this command applies only to the LANE Configuration Server (LECS). This keyword indicates that the LECS should use the 20-byte address that you explicitly entered.
	<i>atm-address-template</i>	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the ESI bytes, or the selector byte of the automatically assigned ATM address.

## lane config database

To associate a named configuration table (database) with the configuration server on the selected ATM interface, use the **lane config database** command in interface configuration mode. To remove the association between a named database and the configuration server on the specified interface, use the **no** form of this command.

**lane config database** *database-name*

**no lane config database**

<b>Syntax Description</b>	<i>database-name</i>	Name of the LANE database.
---------------------------	----------------------	----------------------------

## lane database

To create a named configuration database that can be associated with a configuration server, use the **lane database** command in global configuration mode. To delete the database, use the **no** form of this command.

**lane database** *database-name*

**no lane database** *database-name*

<b>Syntax Description</b>	<i>database-name</i>	Database name (32 characters maximum).
---------------------------	----------------------	--

## lane fixed-config-atm-address

To specify that the fixed configuration server ATM address assigned by the ATM Forum will be used, use the **lane fixed-config-atm-address** command in interface configuration mode. To specify that the fixed ATM address will not be used, use the **no** form of this command.

**lane [config] fixed-config-atm-address**

**no lane [config] fixed-config-atm-address**

---

**Syntax Description**

---

<b>config</b>	(Optional) When the <b>config</b> keyword is used, this command applies only to the LANE Configuration Server (LECS). This keyword indicates that LECS should use the well-known, ATM Forum LEC address.
---------------	--

---

## lane fssrp

To enable the special LANE features such that LANE components (such as the LANE Configuration Server, the LANE client, the LANE server, and the BUS) become aware of FSSRP, use the **lane fssrp** command in interface configuration mode. To disable the LANE FSSRP configuration, use the **no** form of this command.

**lane fssrp**

**no lane fssrp**

---

**Syntax Description**

This command contains no keywords or arguments.





## Switching Services Commands: **lane global-lecs-address** Through **show interface stats**

---

This chapter describes the function and syntax of the switching services commands: **lane global-lecs-address** through **show interface stats**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Switching Services Command Reference*.

### **lane global-lecs-address**

To specify a list of LECS addresses to use when the addresses cannot be obtained from the ILMI, use the **lane global-lecs-address** command in interface configuration mode. To remove a LECS address from the list, use the **no** form of this command.

**lane global-lecs-address** *address*

**no lane global-lecs-address** *address*

---

#### **Syntax Description**

<i>address</i>	Address of the LECS. You cannot use the well-known LECS address.
----------------	--

---

### **lane le-arp**

To add a static entry to the LE ARP table of the LANE client configured on the specified subinterface, use the **lane le-arp** command in interface configuration mode. To remove a static entry from the LE ARP table of the LANE client on the specified subinterface, use the **no** form of this command.

**lane le-arp** {*mac-address* | **route-desc segment** *segment-number* **bridge** *bridge-number*}  
*atm-address*

**no lane le-arp** {*mac-address* | **route-desc segment** *segment-number* **bridge** *bridge-number*}  
*atm-address*

<b>Syntax Description</b>	<i>mac-address</i>	MAC address to bind to the specified ATM address.
	<b>route-desc segment</b> <i>segment-number</i>	LANE segment number. The segment number ranges from 1 to 4095.
	<b>bridge</b> <i>bridge-number</i>	Bridge number that is contained in the route descriptor. The bridge number ranges from 1 to 15.
	<i>atm-address</i>	ATM address.

## lane server-atm-address

To specify an ATM address—and thus override the automatic ATM address assignment—for the LANE server on the specified subinterface, use the **lane server-atm-address** command in interface configuration mode. To remove the ATM address previously specified for the LANE server on the specified subinterface and thus revert to the automatic address assignment, use the **no** form of this command.

**lane server-atm-address** *atm-address-template*

**no lane server-atm-address** [*atm-address-template*]

<b>Syntax Description</b>	<i>atm-address-template</i>	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the ESI bytes, or the selector byte of the automatically assigned ATM address.
---------------------------	-----------------------------	---

## lane server-bus

To enable a LANE server and a broadcast and unknown server (BUS) on the specified subinterface with the ELAN ID, use the **lane server-bus** command in interface configuration mode. To disable a LANE server and BUS on the specified subinterface, use the **no** form of this command.

**lane server-bus** {**ethernet** | **tokenring**} *elan-name* [**elan-id** *id*]

**no lane server-bus** {**ethernet** | **tokenring**} *elan-name* [**elan-id** *id*]

<b>Syntax Description</b>	<b>ethernet</b>	Identifies the emulated LAN (ELAN) attached to this subinterface as an Ethernet ELAN.
	<b>tokenring</b>	Identifies the ELAN attached to this subinterface as a Token Ring ELAN.
	<i>elan-name</i>	Name of the ELAN. The maximum length of the name is 32 characters.
	<b>elan-id</b>	(Optional) Identifies the ELAN.
	<i>id</i>	(Optional) Specifies the ELAN ID of the LEC.

## list

To show all or part of the explicit path or paths, use the **list** IP explicit path configuration command.

**list** [*starting-index-number*]

<b>Syntax Description</b>	<i>starting-index-number</i>	Index number at which the explicit path(s) will start to be displayed. Valid values are from 1 to 65535.
---------------------------	------------------------------	--

## mask destination

To specify the destination mask, use the **mask destination** destination-prefix aggregation cache configuration command. To disable the destination mask, use the **no** form of this command.

**mask destination minimum** *value*

**no mask destination minimum** *value*

<b>Syntax Description</b>	<b>minimum</b>	Configures the minimum value for the mask.
	<i>value</i>	Specifies the value for the mask. Range is from 1 to 32.

## mask source

To specify the source mask, use the **mask source** source-prefix aggregation cache configuration command. To disable the source mask, use the **no** form of this command.

**mask source minimum** *value*

**no mask source minimum** *value*

<b>Syntax Description</b>	<b>minimum</b>	Configures the minimum value for the mask.
	<i>value</i>	Specifies the value for the mask. Range is from 1 to 32.

## maximum routes

To limit the maximum number of routes in a VRF to prevent a PE router from importing too many routes, use the **maximum routes** command in VRF configuration submode. To remove the limit on the maximum number of routes allowed, use the **no** form of this command.

**maximum routes** *limit* {*warn threshold* | **warn-only**}

**no maximum routes**

Syntax Description		
	<i>limit</i>	Specifies the maximum number of routes allowed in a VRF. You may select from 1 to 4,294,967,295 routes to be allowed in a VRF.
	<i>warn threshold</i>	Rejects routes when the threshold limit is reached. The threshold limit is a percentage of the limit specified, from 1 to 100.
	<b>warn-only</b>	Issues a syslog error message when the maximum number of routes allowed for a VRF exceeds the threshold. However, additional routes are still allowed.

## metric-style narrow

To configure a router running IS-IS so that it generates and accepts old-style type, length, and value objects (TLVs), use the **metric-style narrow** router configuration command. To disable this feature, use the **no** form of this command.

```
metric-style narrow [transition] [ { level-1 | level-2 | level-1-2 } ]
```

```
no metric-style narrow [transition] [ { level-1 | level-2 | level-1-2 } ]
```

Syntax Description		
	<b>transition</b>	(Optional) Instructs the router to use both old- and new-style TLVs.
	<b>level-1</b>	(Optional) Enables this command on routing level 1.
	<b>level-2</b>	(Optional) Enables this command on routing level 2.
	<b>level-1-2</b>	(Optional) Enables this command on routing levels 1 and 2.

## metric-style transition

To configure a router running IS-IS so that it generates and accepts both old-style and new-style type, length, and value objects (TLVs), use the **metric-style transition** router configuration command. To disable this feature, use the **no** form of this command.

```
metric-style transition [{level-1 | level-2 | level-1-2}]
```

```
no metric-style transition [{level-1 | level-2 | level-1-2}]
```

Syntax Description		
	<b>level-1</b>	(Optional) Enables this command on routing level 1.
	<b>level-2</b>	(Optional) Enables this command on routing level 2.
	<b>level-1-2</b>	(Optional) Enables this command on routing levels 1 and 2.

## metric-style wide

To configure a router running IS-IS so that it generates and accepts only new-style type, length, and value objects (TLVs), use the **metric-style wide** router configuration command. To disable this feature, use the **no** form of this command.

```
metric-style wide [transition][{level-1 | level-2 | level-1-2}]
```

```
no metric-style wide [transition][{level-1 | level-2 | level-1-2}]
```

### Syntax Description

<b>transition</b>	(Optional) Instructs the router to accept both old- and new-style TLVs.
<b>level-1</b>	(Optional) Enables this command on routing level 1.
<b>level-2</b>	(Optional) Enables this command on routing level 2.
<b>level-1-2</b>	(Optional) Enables this command on routing levels 1 and 2.

## mls rp ip

To enable Multilayer Switching Protocol (MLSP), use the **mls rp ip** command in global configuration mode. To disable MLS, use the **no** form of this command.

```
mls rp ip
```

```
no mls rp ip
```

### Syntax Description

There are no arguments or keywords for this command.

## mls rp ip multicast

To enable IP multicast Multilayer Switching (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000, use the **mls rp ip multicast** command in interface configuration mode. To disable IP multicast Multilayer Switching (MLS) on the interface or VLAN, use the **no** form of this command.

```
mls rp ip multicast
```

```
no mls rp ip multicast
```

### Syntax Description

This command has no arguments or keywords.

## mls rp ip multicast management-interface

To assign a different interface (other than the default) to act as the management interface for Multilayer Switching Protocol (MLSP), use the **mls rp ip multicast management-interface** command in interface configuration mode. To restore the default interface as the management interface, use the **no** form of this command.

```
mls rp ip multicast management-interface
```

```
no mls rp ip multicast management-interface
```

---

**Syntax Description** This command has no arguments or keywords.

## mls rp ipx (global)

To enable the router as an IPX Multilayer Switching (MLS) Route Processor (RP), use the **mls rp ipx** command in global configuration. To disable IPX MLS on the router, use the **no** form of this command.

```
mls rp ipx
```

```
no mls rp ipx
```

---

**Syntax Description** This command has no arguments or keywords.

## mls rp ipx (interface)

To enable IPX MLS on a router interface, use the **mls rp ipx** command in interface configuration mode. To disable IPX MLS on a router interface, use the **no** form of this command.

```
mls rp ipx
```

```
no mls rp ipx
```

---

**Syntax Description** This command has no arguments or keywords.

## mls rp locate ipx

To display information about all switches currently shortcutting for the specified IPX flows, use the **mls rp locate ipx** command in privileged EXEC mode.

```
mls rp locate ipx destination-network.destination-node [source-network]
```

<b>Syntax Description</b>	<i>destination-network.destination-node</i>	The destination network and destination node of IPX packet flows. The destination network consists of 1 to 8 hexadecimal numbers in the format xxxxxxxx. The destination node consists of 1 to 12 hexadecimal numbers in the format xxxx.xxxx.xxxx.
	<i>source-network</i>	(Optional) The source network of the IPX flow. The source network consists of 1 to 8 hexadecimal numbers in the format yyyyyyyy.

## mls rp management-interface

To specify an interface as the management interface, use the **mls rp management-interface** command in interface configuration mode. To remove an interface as the management interface, use the **no** form of this command.

**mls rp management-interface**

**no mls rp management-interface**

**Syntax Description** This command has no keywords or arguments.

## mls rp nde-address

To specify a NetFlow Data Export address, use the **mls rp nde-address** command in global configuration mode.

**mls rp nde-address** *ip-address*

**Syntax Description** *ip-address* NDE IP address.

## mls rp vlan-id

To assign a virtual LAN (VLAN) identification number to an IPX MLS interface, use the **mls rp vlan-id** command in interface configuration mode. To remove a VLAN identification number, use the **no** form of this command.

**mls rp vlan-id** *vlan-id-number*

**no mls rp vlan-id** *vlan-id-number*

**Syntax Description** *vlan-id-number* A VLAN identification number from 1 to 4096.

## mls rp vtp-domain

To assign a Multilayer Switching (MLS) interface to a specific Virtual Trunk Protocol (VTP) domain on the MLS Route Processor (RP), use the **mls rp vtp-domain** command in interface configuration mode. To remove a VTP domain, use the **no** form of this command.

**mls rp vtp-domain** *domain-name*

**no mls rp vtp-domain** *domain-name*

### Syntax Description

<i>domain-name</i>	The name of the VTP domain assigned to an MLS interface and its related switches.
--------------------	---

## mpls atm control-vc

To configure the VPI and VCI to be used for the initial link to the label switching peer device, use the **mpls atm control-vc** interface configuration command. To clear the interface configuration, use the **no** form of this command.

**mpls atm control-vc** *vpi vci*

**no mpls atm control-vc** *vpi vci*

### Syntax Description

<i>vpi</i>	Virtual path identifier.
<i>vci</i>	Virtual channel identifier.

## mpls atm vpi

To configure the range of values to be used in the VPI field for label VCs, use the **mpls atm vpi** interface configuration command. To clear the interface configuration, use the **no** form of this command.

**mpls atm vpi** *vpi* [- *vpi*]

**no mpls atm vpi** *vpi* [- *vpi*]

### Syntax Description

<i>vpi</i>	Virtual path identifier (low end of range).
- <i>vpi</i>	(Optional) Virtual path identifier (high end of range).

## mpls ip (global configuration)

To enable MPLS forwarding of IPv4 packets along normally routed paths for the platform, use the **mpls ip** global configuration command. To disable this feature, use the **no** form of this command.

**mpls ip**

**no mpls ip**

**Syntax Description** This command has no arguments or keywords.

## mpls ip (interface configuration)

To enable MPLS forwarding of IPv4 packets along normally routed paths for a particular interface, use the **mpls ip** interface configuration command. To disable this feature, use the **no** form of this command.

**mpls ip**

**no mpls ip**

**Syntax Description** This command has no arguments or keywords.

## mpls ip default-route

To enable the distribution of labels associated with the IP default route, use the **mpls ip default-route** global configuration command.

**mpls ip default-route**

**Syntax Description** This command has no arguments or keywords.

## mpls ip propagate-ttl

To control the generation of the time to live (TTL) field in the MPLS header when labels are first added to an IP packet, use the **mpls ip propagate-ttl** global configuration command. To use a fixed TTL value (255) for the first label of the IP packet, use the **no** form of this command.

**mpls ip propagate-ttl**

**no mpls ip propagate-ttl [forwarded | local]**

<b>Syntax Description</b>	<b>forwarded</b>	(Optional) Prevents the <b>traceroute</b> command from showing the hops for forwarded packets.
	<b>local</b>	(Optional) Prevents the <b>traceroute</b> command from showing the hops only for local packets.

## mpls ip ttl-expiration pop

To specify how a packet with an expired time to live (TTL) value is forwarded, use the **mpls ip ttl-expiration pop** privileged EXEC command. To disable this feature, use the **no** form of the command.

**mpls ip ttl-expiration pop** *labels*

**no mpls ip ttl-expiration pop** *labels*

<b>Syntax Description</b>	<i>labels</i>	The maximum number of labels in the packet necessary for the packet to be forwarded by means of the global IP routing table.
---------------------------	---------------	--

## mpls label range

To configure the range of local labels available for use on packet interfaces, use the **mpls label range** global configuration command. To revert to the platform defaults, use the **no** form of this command.

**mpls label range** *min max*

**no mpls label range**

<b>Syntax Description</b>	<i>min</i>	The smallest label allowed in the label space. The default is 16.
	<i>max</i>	The largest label allowed in the label space. The default is 1048575.

## mpls mtu

To set the per-interface maximum transmission unit (MTU) for labeled packets, use the **mpls mtu** interface configuration command.

**mpls mtu** *bytes*

**no mpls mtu**

<b>Syntax Description</b>	<i>bytes</i>	The MTU value (in bytes). The minimum allowable value is 64; the maximum allowable value is interface dependent.
---------------------------	--------------	--

## mpls netflow egress

To enable MPLS egress NetFlow accounting on an interface, use the **mpls netflow egress** interface configuration command. To disable MPLS egress NetFlow accounting, use the **no** form of this command.

**mpls netflow egress**

**no mpls netflow egress**

---

**Syntax Description** This command has no arguments or keywords.

## mpls traffic-eng

To configure a router running IS-IS so that it floods MPLS traffic engineering link information into the indicated IS-IS level, use the **mpls traffic-eng** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng {level-1 | level-2}**

**no mpls traffic-eng {level-1 | level-2}**

---

<b>Syntax Description</b>	<b>level-1</b>	Floods MPLS traffic engineering link information into IS-IS level 1.
	<b>level-2</b>	Floods MPLS traffic engineering link information into IS-IS level 2.

---

## mpls traffic-eng administrative-weight

To override the Interior Gateway Protocol (IGP) administrative weight (cost) of the link, use the **mpls traffic-eng administrative-weight** interface configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng administrative-weight *weight***

**no mpls traffic-eng administrative-weight**

---

<b>Syntax Description</b>	<i>weight</i>	Cost of the link.
---------------------------	---------------	-------------------

---

## mpls traffic-eng administrative-weight

To override the Interior Gateway Protocol (IGP) administrative weight (cost) of the link, use the **mpls traffic-eng administrative-weight** interface configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng administrative-weight** *weight*

**no mpls traffic-eng administrative-weight**

Syntax Description	<i>weight</i>	Cost of the link.
--------------------	---------------	-------------------

## mpls traffic-eng area

To configure a router running Open Shortest Path First (OSPF) MPLS so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng area** *num*

**no mpls traffic-eng area** *num*

Syntax Description	<i>num</i>	The OSPF area on which MPLS traffic engineering is enabled.
--------------------	------------	---

## mpls traffic-eng attribute-flags

To set the user-specified attribute flags for the interface, use the **mpls traffic-eng attribute-flags** interface configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng attribute-flags** *attributes*

**no mpls traffic-eng attribute-flags**

Syntax Description	<i>attributes</i>	Links attributes that will be compared to a tunnel's affinity bits during selection of a path.  Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.
--------------------	-------------------	---

## mpls traffic-eng flooding thresholds

To set a link's reserved bandwidth thresholds, use the **mpls traffic-eng flooding thresholds** interface configuration command. To return to the default settings, use the **no** form of this command.

**mpls traffic-eng flooding thresholds** { **down** | **up** } *percent* [*percent* ...]

**no mpls traffic-eng flooding thresholds** { **down** | **up** }

Syntax Description		
	<b>down</b>	Sets the thresholds for decreased resource availability.
	<b>up</b>	Sets the thresholds for increased resource availability.
	<i>percent</i> [ <i>percent</i> ]	Bandwidth threshold level. For the <b>down</b> keyword, valid values are from 0 through 99. For the <b>up</b> keyword, valid values are from 1 through 100.

## mpls traffic-eng link-management timers bandwidth-hold

To set the length of time that bandwidth is held for an RSVP path (setup) message while you wait for the corresponding RSVP Resv message to come back, use the **mpls traffic-eng link-management timers bandwidth-hold** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng link-management timers bandwidth-hold** *hold-time*

**no mpls traffic-eng link-management timers bandwidth-hold**

Syntax Description		
	<i>hold-time</i>	Length of time that bandwidth can be held. Valid values are from 1 to 300 seconds.

## mpls traffic-eng link-management timers periodic-flooding

To set the length of the interval for periodic flooding, use the **mpls traffic-eng link-management timers periodic-flooding** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng link-management timers periodic-flooding** *interval*

**no mpls traffic-eng link-management timers periodic-flooding**

Syntax Description		
	<i>interval</i>	Length of the interval (in seconds) for periodic flooding. Valid values are from 0 to 3600. A value of 0 turns off periodic flooding. If you set this value from 1 to 29, it is treated as 30.

## mpls traffic-eng link timers bandwidth-hold

To set the length of time that bandwidth is “held” for a RSVP PATH (Set Up) message while waiting for the corresponding RSVP RESV message to come back, use the **mpls traffic-eng link timers bandwidth-hold** command in global configuration mode.

```
mpls traffic-eng link timers bandwidth-hold hold-time
```

<b>Syntax Description</b>	<i>hold-time</i>	Sets the length of time that bandwidth can be held. The range is from 1 to 300 seconds.
---------------------------	------------------	---

## mpls traffic-eng link timers periodic-flooding

To set the length of the interval used for periodic flooding, use the **mpls traffic-eng link timers periodic-flooding** command in global configuration mode.

```
mpls traffic-eng link timers periodic-flooding interval
```

<b>Syntax Description</b>	<i>interval</i>	Length of interval used for periodic flooding (in seconds). The range is from 0 to 3600. If you set this value to 0, you turn off periodic flooding. If you set this value anywhere in the range from 1 to 29, it is treated as 30.
---------------------------	-----------------	---

## mpls traffic-eng logging lsp

To log certain traffic engineering label-switched path (LSP) events, use the **mpls traffic-eng logging lsp** router configuration command. To disable this feature, use the **no** form of this command.

```
mpls traffic-eng logging lsp { path-errors | reservation-errors | preemption | setups | teardowns } [aclnum]
```

```
no mpls traffic-eng logging lsp { path-errors | reservation-errors | preemption | setups | teardowns } [aclnum]
```

<b>Syntax Description</b>	<b>path-errors</b>	Logs RSVP path errors for traffic engineering LSPs.
	<b>reservation-errors</b>	Logs RSVP reservation errors for traffic engineering LSPs.
	<b>preemption</b>	Logs events related to the preemption of traffic engineering LSPs.
	<b>setups</b>	Logs events related to the establishment of traffic engineering LSPs.
	<b>teardowns</b>	Logs events related to the removal of traffic engineering LSPs.
	<i>aclnum</i>	(Optional) Uses the specified access list to filter the events that are logged. Logs events only for LSPs that match the access list.

## mpls traffic-eng logging tunnel

To log certain traffic engineering tunnel events, use the **mpls traffic-eng logging tunnel** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng logging tunnel lsp-selection** [*aclnum*]

**no mpls traffic-eng logging tunnel lsp-selection** [*aclnum*]

Syntax Description		
	<b>lsp-selection</b>	Logs events related to the selection of an LSP for a traffic engineering tunnel.
	<i>aclnum</i>	(Optional) Uses the specified access list to filter the events that are logged. Logs events only for tunnels that match the access list.

## mpls traffic-eng reoptimize

To force immediate reoptimization of all traffic engineering tunnels, use the **mpls traffic-eng reoptimize EXEC** command.

**mpls traffic-eng reoptimize**

Syntax Description	
	This command has no arguments or keywords.

## mpls traffic-eng reoptimize events

To turn on automatic reoptimization of MPLS traffic engineering when certain events occur, such as when an interface becomes operational, use the **mpls traffic-eng reoptimize events** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng reoptimize events** {**link-up**}

**no mpls traffic-eng reoptimize events** {**link-up**}

Syntax Description		
	<b>link-up</b>	Triggers automatic reoptimization whenever an interface becomes operational.

## mpls traffic-eng reoptimize timers frequency

To control the frequency with which tunnels with established label-switched paths (LSPs) are checked for better LSPs, use the **mpls traffic-eng reoptimize timers frequency** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng reoptimize timers frequency** *seconds*

**no mpls traffic-eng reoptimize timers frequency**

<b>Syntax Description</b>	<i>seconds</i>	Sets the frequency of reoptimization (in seconds). A value of 0 disables reoptimization.
---------------------------	----------------	--

## mpls traffic-eng router-id

To specify that the traffic engineering router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng router-id** *interface-name*

**no mpls traffic-eng router-id**

<b>Syntax Description</b>	<i>interface-name</i>	Interface whose primary IP address is the router's identifier.
---------------------------	-----------------------	--

## mpls traffic-eng signalling advertise implicit-null

To use MPLS encoding for the implicit-null label in signalling messages sent to neighbors that match the specified access list, use the **mpls traffic-eng signalling advertise implicit-null** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng signalling advertise implicit-null** [*aclname* | *aclnum*]

**no mpls traffic-eng signalling advertise implicit-null**

<b>Syntax Description</b>	<i>aclname</i>	Name of the access list.
	<i>aclnum</i>	Number of the access list.

## mpls traffic-eng tunnels (configuration)

To enable MPLS traffic engineering tunnel signaling on a device, use the **mpls traffic-eng tunnels** router configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng tunnels**

**no mpls traffic-eng tunnels**

---

**Syntax Description** This command has no arguments or keywords.

## mpls traffic-eng tunnels (interface)

To enable MPLS traffic engineering tunnel signalling on an interface (assuming that it is enabled on the device), use the **mpls traffic-eng tunnels** interface configuration command. To disable this feature, use the **no** form of this command.

**mpls traffic-eng tunnels**

**no mpls traffic-eng tunnels**

---

**Syntax Description** This command has no arguments or keywords.

## mposa client config name

To define an MPC with a specified name, use the **mposa client config name** command in global configuration mode. To delete the MPC, use the **no** form of this command.

**mposa client config name** *mpc-name*

**no mposa client config name** *mpc-name*

---

**Syntax Description** *mpc-name* Specifies the name of an MPC.

---

## mposa client name

To attach an MPC to a major ATM interface, use the **mposa client name** command in interface configuration mode. To break the attachment, use the **no** form of this command.

**mposa client name** *mpc-name*

**no mposa client name** *mpc-name*

---

**Syntax Description** *mpc-name* Specifies the name of an MPC.

---

## mpoa server config name

To define an MPS with the specified name, use the **mpoa server config name** command in global configuration mode. To delete an MPS, use the **no** form of this command.

**mpoa server config name** *mps-name*

**no mpoa server config name** *mps-name*

Syntax Description	<i>mps-name</i>	Name of the MPOA server.
--------------------	-----------------	--------------------------

## mpoa server name

To attach an MPS to a major ATM interface, use the **mpoa server name** command in interface configuration mode. To break the attachment, use the **no** form of this command.

**mpoa server name** *mps-name*

**no mpoa server name** *mps-name*

Syntax Description	<i>mps-name</i>	Name of the MPOA server.
--------------------	-----------------	--------------------------

## mpoa server name trigger ip-address

To originate an MPOA trigger for the specified IP address to the specified MPOA client from the specified MPS, use the **mpoa server name trigger ip-address** interface configuration command.

**mpoa server name** *mps-name* **trigger ip-address** *ip address* [**mpc-address** *mpc-address*]

Syntax Description	<i>mps-name</i>	Specifies the name of the MPOA server.
	<i>ip address</i>	Specifies the IP address.
	<b>mpc-address</b> <i>mpc-address</i>	(Optional) Specifies the MPOA client (MPC) address to which the trigger should be sent. If the address is not specified, a trigger will be sent to all clients.

## name elan-id

To configure the emulated LAN (ELAN) ID of an ELAN in the LECS database to participate in MPOA, use the **name elan-id** command in LANE database configuration mode. To disable the ELAN ID of an ELAN in the LECS database to participate in MPOA, use the **no** form of this command.

**name** *name* **elan-id** *id*

**no name** *name* **elan-id** *id*

### Syntax Description

<i>name</i>	Specifies the name of the ELAN.
<i>id</i>	Specifies the identification number of the ELAN.

## name local-seg-id

To specify or replace the ring number of the emulated LAN (ELAN) in the configuration server's configuration database, use the **name local-seg-id** command in database configuration mode. To remove the ring number from the database, use the **no** form of this command.

**name** *elan-name* **local-seg-id** *segment-number*

**no name** *elan-name* **local-seg-id** *segment-number*

### Syntax Description

<i>elan-name</i>	Name of the ELAN. The maximum length of the name is 32 characters.
<i>segment-number</i>	Segment number to be assigned to the ELAN. The number ranges from 1 to 4095.

## name preempt

To set the emulated LAN (ELAN) preempt, use the **name preempt** command in LANE database configuration mode. To disable preemption, use the **no** form of this command.

**name** *elan-name* **preempt**

**no name** *elan-name* **preempt**

### Syntax Description

<i>elan-name</i>	Specifies the name of the ELAN.
------------------	---------------------------------

## name server-atm-address

To specify or replace the ATM address of the LANE server for the emulated LAN (ELAN) in the configuration server's configuration database, use the **name server-atm-address** command in database configuration mode. To remove it from the database, use the **no** form of this command.

**name** *elan-name* **server-atm-address** *atm-address* [**restricted** | **un-restricted**] [*index number*]

**no name** *elan-name* **server-atm-address** *atm-address* [**restricted** | **un-restricted**] [*index number*]

### Syntax Description

<i>elan-name</i>	Name of the ELAN. Maximum length is 32 characters.
<i>atm-address</i>	LANE server's ATM address.
<b>restricted</b>   <b>un-restricted</b>	(Optional) Membership in the named ELAN is restricted to the LANE clients explicitly defined to the ELAN in the configuration server's database.
<b>index number</b>	(Optional) Priority number. When specifying multiple LANE servers for fault tolerance, you can specify a priority for each server. 0 is the highest priority.

## neighbor activate

To enable the exchange of information with a neighboring router, use the **neighbor activate** command in address family configuration or router configuration mode. To disable the exchange of an address with a neighboring router, use the **no** form of this command.

**neighbor** {*ip-address* | *peer-group-name*} **activate**

**no neighbor** {*ip-address* | *peer-group-name*} **activate**

### Syntax Description

<i>ip-address</i>	IP address of the neighboring router.
<i>peer-group-name</i>	Name of BGP peer group.

## neighbor allowas-in

To configure PE routers to allow readvertisement of all prefixes containing duplicate ASNs, use the **neighbor allowas-in** command in router configuration mode. To disable the readvertisement of a PE router's ASN, use the **no** form of this command.

**neighbor allowas-in** *number*

**no neighbor allowas-in** *number*

### Syntax Description

<i>number</i>	Specifies the number of times to allow the advertisement of a PE router's ASN. Valid values are from 1 to 10 times.
---------------	---

## neighbor as-override

To configure a PE router to override the ASN of a site with the ASN of a provider, use the **neighbor as-override** command in router configuration mode. To remove VPN IPv4 prefixes from a specified router, use the **no** form of this command.

**neighbor** *ip-address* **as-override**

**no neighbor** *ip-address* **as-override**

<b>Syntax Description</b>	<i>ip-address</i>	Specifies the IP address of the router that is to be overridden with the ASN provided.
---------------------------	-------------------	--

## network-id

To specify the network ID of an MPS, use the **network-id** command in MPS configuration mode. To revert to the default value (default value is 1), use the **no** form of this command.

**network-id** *id*

**no network-id**

<b>Syntax Description</b>	<i>id</i>	Specifies the network ID of the MPOA server.
---------------------------	-----------	--

## next-address

To specify the next IP address in the explicit path, use the **next-address** IP explicit path configuration command. To disable this feature, use the **no** form of this command.

**next-address** *A.B.C.D*

**no next-address** *A.B.C.D*

<b>Syntax Description</b>	<i>A.B.C.D</i>	Next IP address in the explicit path.
---------------------------	----------------	---------------------------------------

# rate-limit

To configure CAR and DCAR policies, use the **rate-limit** interface configuration command. To remove the rate limit from the configuration, use the **no** form of this command.

```
rate-limit {input | output} [access-group [rate-limit] acl-index] bps
    burst-normal burst-max conform-action conform-action exceed-action exceed-action
```

```
no rate-limit {input | output}[access-group [rate-limit] acl-index] bps
    burst-normal burst-max conform-action conform-action exceed-action exceed-action
```

## Syntax Description

<b>input</b>	Applies this CAR traffic policy to packets received on this input interface.
<b>output</b>	Applies this CAR traffic policy to packets sent on this output interface.
<b>access-group</b>	(Optional) Applies this CAR traffic policy to the specified access list.
<b>rate-limit</b>	(Optional) The access list is a rate-limit access list.
<i>acl-index</i>	(Optional) Access list number.
<i>bps</i>	Average rate (in bits per second). The value must be in increments of 8 kbps.
<i>burst-normal</i>	Normal burst size (in bytes). The minimum value is bits per second divided by 2000.
<i>burst-max</i>	Excess burst size (in bytes).
<b>conform-action</b> <i>conform-action</i>	Action to take on packets that conform to the specified rate limit. Specify one of the following keywords: <ul style="list-style-type: none"> <li>• <b>continue</b>—Evaluates the next <b>rate-limit</b> command.</li> <li>• <b>drop</b>—Drops the packet.</li> <li>• <b>set-dscp-continue</b>—Sets the differentiated services code point (DSCP) (0 to 63) and evaluate the next <b>rate-limit</b> command.</li> <li>• <b>set-dscp-transmit</b>—Sends the DSCP and transmit the packet.</li> <li>• <b>set-mpls-exp-continue</b>—Sets the MPLS experimental bits (0 to 7) and evaluates the next <b>rate-limit</b> command.</li> <li>• <b>set-mpls-exp-transmit</b>—Sets the MPLS experimental bits (0 to 7) and sends the packet.</li> <li>• <b>set-prec-continue</b>—Sets the IP precedence (0 to 7) and evaluates the next <b>rate-limit</b> command.</li> <li>• <b>set-prec-transmit</b>—Sets the IP precedence (0 to 7) and sends the packet.</li> <li>• <b>set-qos-continue</b>—Sets the QoS group ID (1 to 99) and evaluates the next <b>rate-limit</b> command.</li> <li>• <b>set-qos-transmit</b>—Sets the QoS group ID (1 to 99) and sends the packet.</li> <li>• <b>transmit</b>—Sends the packet.</li> </ul>

<b>exceed-action</b> <i>exceed-action</i>	<p>Action to take on packets that exceed the specified rate limit. Specify one of the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>continue</b>—Evaluates the next <b>rate-limit</b> command.</li> <li>• <b>drop</b>—Drops the packet.</li> <li>• <b>set-dscp-continue</b>—Sets the DSCP (0 to 63) and evaluates the next <b>rate-limit</b> command.</li> <li>• <b>set-dscp-transmit</b>—Sends the DSCP and sends the packet.</li> <li>• <b>set-mpls-exp-continue</b>—Sets the MPLS experimental bits (0 to 7) and evaluates the next <b>rate-limit</b> command.</li> <li>• <b>set-mpls-exp-transmit</b>—Sets the MPLS experimental bits (0 to 7) and sends the packet.</li> <li>• <b>set-prec-continue</b>—Sets the IP precedence (0 to 7) and evaluates the next <b>rate-limit</b> command.</li> <li>• <b>set-prec-transmit</b>—Sets the IP precedence (0 to 7) and sends the packet.</li> <li>• <b>set-qos-continue</b>—Sets the QoS group ID (1 to 99) and evaluates the next <b>rate-limit</b> command.</li> <li>• <b>set-qos-transmit</b>—Sets the QoS group ID (1 to 99) and sends the packet.</li> <li>• <b>transmit</b>—Sends the packet.</li> </ul>
---	--

## rd

To create routing and forwarding tables for a VRF, use the **rd** command in VRF configuration submode.

```
rd route-distinguisher
```

<b>Syntax Description</b>	<i>route-distinguisher</i>	Adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.
---------------------------	----------------------------	---

## route-target

To create a route-target extended community for a VRF, use the **route-target** command in VRF configuration submode. To disable the configuration of a route-target community option, use the **no** form of this command.

```
route-target {import | export | both} route-target-ext-community
```

```
no route-target {import | export | both} route-target-ext-community
```

<b>Syntax Description</b>	<b>import</b>	Imports routing information from the target VPN extended community.
	<b>export</b>	Exports routing information to the target VPN extended community.

<b>both</b>	Imports both import and export routing information to the target VPN extended community.
<i>route-target-ext-community</i>	Adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.

## set ip next-hop verify-availability

To configure policy routing to verify that the next hops of a route map is a CDP neighbor before policy routing to that next hop, use the **set ip next-hop verify-availability** route-map configuration command.

**set ip next-hop verify-availability**

**Syntax Description** This command has no arguments or keywords.

## set mpls experimental

To configure a policy to set the MPLS experimental field within the modular QoS command-line interface (CLI), use the **set mpls experimental** policy-map configuration command. To disable the policy map, use the **no** form of this command.

**set mpls experimental** *value*

**no set mpls experimental** *value*

**Syntax Description** *value* Specifies the value used to set MPLS experimental bits defined by the policy map. Valid values are 0 to 7, and they can be space-delimited. For example, 3 4 7.

## set ospf router-id

To set a separate OSPF router ID for each interface or subinterface on a PE router for each directly attached CE router, use the **set ospf router-id** command in route-map configuration mode.

**set ospf router-id**

**Syntax Description** This command has no arguments or keywords.

## shortcut-frame-count

To specify the maximum number of times a packet can be routed to the default router within shortcut-frame time before an MPOA resolution request is sent, use the **shortcut-frame-count** command in MPC configuration mode. To restore the default shortcut-setup frame count value, use the **no** form of this command.

**shortcut-frame-count** *count*

**no shortcut-frame-count**

<b>Syntax Description</b>	<i>count</i>	Shortcut-setup frame count. The default is 10 frames.
---------------------------	--------------	---

## shortcut-frame-time

To set the shortcut-setup frame time (in seconds) for the MPC, use the **shortcut-frame-time** command in MPC configuration mode. To restore the default shortcut-setup frame-time value, use the **no** form of this command.

**shortcut-frame-time** *time*

**no shortcut-frame-time**

<b>Syntax Description</b>	<i>time</i>	Shortcut-setup frame time (in seconds).
---------------------------	-------------	---

## show adjacency

To display Cisco Express Forwarding (CEF) adjacency table information, use the **show adjacency** command in EXEC mode.

**show adjacency** [**detail**]

<b>Syntax Description</b>	<b>detail</b>	(Optional) Displays detailed adjacency information, including Layer 2 information.
---------------------------	---------------	--

## show atm vc

To display information about private ATM virtual circuits (VCs), use the following **show atm vc** privileged EXEC command.

**show atm vc** [*vcd*]

<b>Syntax Description</b>	<i>vcd</i>	(Optional) Specifies the VC to display information about.
---------------------------	------------	---

## show cable bundle

To display the forwarding table for the specified interface, use the **show cable bundle** privileged EXEC command.

```
show cable bundle bundle-number forwarding-table
```

Syntax Description		
	<i>bundle-number</i>	Specifies the bundle identifier. Valid range is from 1 to 255.
	<i>forwarding-table</i>	Displays the forwarding table for the specified interface.

## show cef

To display which packets the line cards dropped or to display which packets were not express forwarded, use the **show cef** command in EXEC mode.

```
show cef [drop | not-cef-switched]
```

Syntax Description		
	<b>drop</b>	(Optional) Displays which packets were dropped by each line card.
	<b>not-cef-switched</b>	(Optional) Displays which packets were sent to a different switching path.

## show cef interface

To display detailed Cisco Express Forwarding (CEF) information for all interfaces, use the **show cef interface** command in EXEC mode.

```
show cef interface [type number]
```

Syntax Description		
	<i>type number</i>	(Optional) Displays detailed CEF information for the specified interface type and number.

## show cef linecard

To display Cisco Express Forwarding (CEF)-related interface information by line card, use the **show cef linecard** command in EXEC mode.

```
show cef linecard [slot-number] [detail]
```

Syntax Description		
	<i>slot-number</i>	(Optional) Slot number containing the line card about which to display CEF-related information. When you omit this argument, information about all line cards is displayed.
	<b>detail</b>	(Optional) Displays detailed CEF information for the specified line card.

## show controllers vsi control-interface

To display information about an ATM interface configured with the **tag-control-protocol vsi EXEC** command to control an external switch (or if an interface is not specified, to display information about all VSI control interfaces), use the **show controllers vsi control-interface** command.

```
show controllers vsi control-interface [interface]
```

Syntax Description	
	<i>interface</i> (Optional) Specifies the interface number.

## show controllers vsi descriptor

To display information about a switch interface discovered by the MPLS LSC through VSI, or if no descriptor is specified, about all such discovered interfaces, use the **show controllers vsi descriptor EXEC** command.

```
show controllers vsi descriptor [descriptor]
```

Syntax Description	
	<i>descriptor</i> (Optional) Physical descriptor. For the Cisco BPX switch, the physical descriptor has the following form: <i>slot.port.0</i>

## show controllers vsi session

To display information about all sessions with VSI slaves, use the **show controllers vsi session EXEC** command.

```
show controllers vsi session [session-num [interface interface]]
```



### Note

A session consists of an exchange of VSI messages between the VSI master (the LSC) and a VSI slave (an entity on the switch). There can be multiple VSI slaves for a switch. On the BPX, each port or trunk card assumes the role of a VSI slave.

Syntax Description	
	<i>session-num</i> (Optional) Specifies the session number.
	<b>interface</b> <i>interface</i> (Optional) Specifies the VSI control interface.

## show controllers vsi status

To display a one-line summary of each VSI-controlled interface, use the `show controllers vsi status EXEC` command.

```
show controllers vsi status
```

---

**Syntax Description** This command has no arguments or keywords.

## show controllers vsi traffic

To display traffic information about VSI-controlled interfaces, VSI sessions, or VCs on VSI-controlled interfaces, use the `show controllers vsi traffic EXEC` command.

```
show controllers vsi traffic [{descriptor descriptor | session session-num | vc [descriptor
descriptor [vpi vci]]}]
```

---

<b>Syntax Description</b>	<b>descriptor</b> <i>descriptor</i>	(Optional) Specifies the interface.
	<b>session</b> <i>session-num</i>	(Optional) Specifies a session number.
	<b>vc</b>	(Optional) Virtual circuit.
	<i>vpi</i>	(Optional) Virtual path identifier.
	<i>vci</i>	(Optional) Virtual circuit identifier.

---

## show controllers XTagATM

To display information about an extended MPLS ATM interface controlled through the VSI protocol (or, if an interface is not specified, to display information about all extended MPLS ATM interfaces controlled through the VSI protocol), use the `show controllers XTagATM EXEC` command.

```
show controllers XTagATM if-num
```

---

<b>Syntax Description</b>	<i>if-num</i>	Specifies the interface number.
---------------------------	---------------	---------------------------------

---

## show interface stats

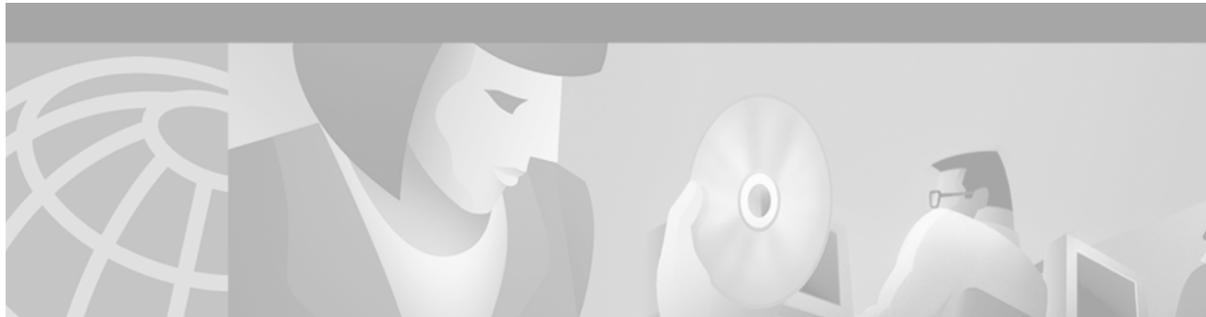
To display numbers of packets that were process switched, fast switched, and distributed switched, use the `show interface stats` command in EXEC mode.

```
show interface type number stats
```

---

<b>Syntax Description</b>	<i>type number</i>	Interface type and number about which to display statistics.
---------------------------	--------------------	--

---



## Switching Services Commands: show interface XTagATM Through tunnel tsp-hop

This chapter describes the function and syntax of the switching services commands: **show interface XTagATM** through **tunnel tsp-hop**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Switching Services Command Reference*.

### show interface XTagATM

To display information about an extended MPLS ATM interface, use the **show interface XTagATM EXEC** command.

```
show interface XTagATM if-num
```

Syntax Description	<i>if-num</i>	Specifies the MPLS ATM interface number.
--------------------	---------------	--

### show ip bgp vpnv4

To display VPN address information from the BGP table, use the **show ip bgp vpnv4** command in EXEC mode.

```
show ip bgp vpnv4 { all | rd route-distinguisher | vrf vrf-name } [ip-prefix/length [longer-prefixes] [output-modifiers]] [network-address [mask] [longer-prefixes] [output-modifiers]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as][neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [tags]
```

Syntax Description	<b>all</b>	Displays the complete VPNv4 database.
	<b>rd</b> <i>route-distinguisher</i>	Displays NLRIs that have a matching route distinguisher.
	<b>vrf</b> <i>vrf-name</i>	Displays NLRIs associated with the named VRF.
	<i>ip-prefix/length</i>	(Optional) IP prefix address (in dotted decimal format) and length of mask (0 to 32).

<b>longer-prefixes</b>	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter, and all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>network-address</i>	(Optional) IP address of a network in the BGP routing table.
<i>mask</i>	(Optional) Mask of the network address, in dotted decimal format.
<b>cidr-only</b>	(Optional) Displays only routes that have nonnatural net masks.
<b>community</b>	(Optional) Displays routes matching this community.
<b>community-list</b>	(Optional) Displays routes matching this community list.
<b>dampened-paths</b>	(Optional) Displays paths suppressed on account of dampening (BGP route from peer is up and down).
<b>filter-list</b>	(Optional) Displays routes conforming to the filter list.
<b>flap-statistics</b>	(Optional) Displays flap statistics of routes.
<b>inconsistent-as</b>	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
<b>neighbors</b>	(Optional) Displays details about TCP and BGP neighbor connections.
<b>paths</b>	(Optional) Displays path information.
<i>line</i>	(Optional) A regular expression to match the BGP AS paths.
<b>peer-group</b>	(Optional) Displays information about peer groups.
<b>quote-regex</b>	(Optional) Displays routes matching the AS path “regular expression.”
<b>regex</b>	(Optional) Displays routes matching the AS path regular expression.
<b>summary</b>	(Optional) Displays BGP neighbor status.
<b>tags</b>	(Optional) Displays incoming and outgoing BGP labels for each NLRI.

## show ip cache

To display the routing table cache used to fast switch IP traffic, use the **show ip cache EXEC** command.

```
show ip cache [prefix mask] [type number]
```

### Syntax Description

<i>prefix</i>	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
<i>mask</i>	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
<i>type</i>	(Optional) Displays only the entries in the cache that match the interface type and number combination.
<i>number</i>	(Optional) Displays only the entries in the cache that match the interface type and number combination.

## show ip cache flow

To display a summary of the NetFlow switching statistics, use the **show ip cache flow** command in EXEC mode.

```
show ip cache flow
```

---

**Syntax Description** This command has no arguments or keywords.

## show ip cache flow aggregation

To display the aggregation cache configuration, use the **show ip cache flow aggregation** command in EXEC mode.

```
show ip cache flow aggregation type
```

---

<b>Syntax Description</b>	<i>type</i>	<p>Displays the configuration of a particular aggregation cache as follows:</p> <ul style="list-style-type: none"> <li>• Autonomous system</li> <li>• Destination prefix</li> <li>• Prefix</li> <li>• Protocol-port</li> <li>• Source prefix</li> </ul>
---------------------------	-------------	---

---

## show ip cef

To display entries in the FIB that are unresolved or to display a summary of the FIB, use the **show ip cef** command in EXEC mode:

```
show ip cef [unresolved | summary]
```

### Specific FIB Entries Based on IP Address Information

```
show ip cef [network [mask [longer-prefix]]] [detail]
```

### Specific FIB Entries Based on Interface Information

```
show ip cef [type number] [detail]
```

---

<b>Syntax Description</b>	<b>unresolved</b>	(Optional) Displays unresolved FIB entries.
	<b>summary</b>	(Optional) Displays a summary of the FIB.

---

<i>network</i>	(Optional) Displays the FIB entry for the specified destination network.
<i>mask</i>	(Optional) Displays the FIB entry for the specified destination network and mask.
<b>longer-prefix</b>	(Optional) Displays FIB entries for more specific destinations.
<b>detail</b>	(Optional) Displays detailed FIB entry information.
<i>type number</i>	(Optional) Interface type and number for which to display FIB entries.

## show ip cef vrf

To display the CEF forwarding table associated with a VRF, use the **show ip cef vrf EXEC** command.

```
show ip cef vrf vrf-name [ip-prefix [mask [longer-prefixes]] [detail] [output-modifiers]] [interface
interface-number] [adjacency [interface interface-number] [detail] [discard] [drop] [glean]
[null] [punt] [output-modifiers]] [detail [output-modifiers]] [non-recursive [detail]
[output-modifiers]] [summary [output-modifiers]] [traffic [prefix-length] [output-modifiers]]
[unresolved [detail] [output-modifiers]]
```

### Syntax Description

<i>vrf-name</i>	Name assigned to the VRF.
<i>ip-prefix</i>	(Optional) IP prefix of entries to show, in dotted decimal format (A.B.C.D).
<i>mask</i>	(Optional) Mask of the IP prefix, in dotted decimal format.
<b>longer-prefixes</b>	(Optional) Displays table entries for more specific routes.
<b>detail</b>	(Optional) Displays detailed information for each CEF table entry.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>interface</i>	(Optional) Type of network interface to use: <b>ATM</b> , <b>Ethernet</b> , <b>Loopback</b> , <b>POS</b> (packet over SONET) or <b>null</b> .
<i>interface-number</i>	(Optional) Number identifying the network interface to use.
<b>adjacency</b>	(Optional) Displays all prefixes resolving through adjacency.
<b>discard</b>	(Optional) Discards adjacency.
<b>drop</b>	(Optional) Drops adjacency.
<b>glean</b>	(Optional) Gleans adjacency.
<b>null</b>	(Optional) Null adjacency.
<b>punt</b>	(Optional) Punts adjacency.
<b>non-recursive</b>	(Optional) Displays only nonrecursive routes.
<b>summary</b>	(Optional) Displays a CEF table summary.
<b>traffic</b>	(Optional) Displays traffic statistics.
<b>prefix-length</b>	(Optional) Displays traffic statistics by prefix size.
<b>unresolved</b>	(Optional) Displays only unresolved routes.

## show ip explicit-paths

To display the configured IP explicit paths, use the **show ip explicit-paths** EXEC command. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

```
show ip explicit-paths [{name word | identifier number}] [detail]
```

Syntax Description	name word	(Optional) Name of the explicit path.
	identifier number	(Optional) Number of the explicit path. Valid values are from 1 to 65535.
	detail	(Optional) Displays, in the long form, information about the configured IP explicit paths.

## show ip flow export

To display the statistics for the data export, including the main cache and all other enabled caches, use the **show ip flow export** command in EXEC mode.

```
show ip flow export
```

**Syntax Description** This command has no keywords and arguments.

## show ip mcache

To display the contents of the IP multicast fast-switching cache, use the **show ip mcache** command in EXEC mode.

```
show ip mcache [group [source]]
```

<b>Syntax Description</b>	group	(Optional) Displays the fast-switching cache for the single group. The <i>group</i> argument can be either a Class D IP address or a DNS name.
	source	(Optional) If the <i>source</i> argument is also specified, displays a single multicast cache entry. The <i>source</i> argument can be either a unicast IP address or a DNS name.

## show ip mds forwarding

On a line card, to display the MFIB table and forwarding information for multicast distributed switching (MDS), use the **show ip mds forwarding** command in EXEC mode.

```
show ip mds forwarding [group-address] [source-address]
```

---

### Syntax Description

<i>group-address</i>	(Optional) Address of the IP multicast group for which to display the MFIB table.
<i>source-address</i>	(Optional) Address of the source of IP multicast packets for which to display the MFIB table.

---

## show ip mds interface

To display the status of multicast distributed switching (MDS) interfaces, use the **show ip mds interface** command in EXEC mode.

```
show ip mds interface
```

---

### Syntax Description

This command has no arguments or keywords.

## show ip mds stats

To display switching statistics or line card statistics for multicast distributed switching (MDS), use the **show ip mds stats** command in EXEC mode.

```
show ip mds stats [switching | linecard]
```

---

### Syntax Description

<b>switching</b>	(Optional) Displays switching statistics.
<b>linecard</b>	(Optional) Displays line card statistics.

---

## show ip mds summary

To display a summary of the MFIB table for multicast distributed switching (MDS), use the **show ip mds summary** command in EXEC mode.

```
show ip mds summary
```

---

### Syntax Description

This command has no arguments or keywords.

## show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** command in EXEC mode.

```
show ip mroute [group-name | group-address] [source] [summary] [count] [active kbps]
```

Syntax Description	
<i>group-name</i>   <i>group-address</i>	(Optional) IP address, name, or interface of the multicast group as defined in the DNS hosts table.
<i>source</i>	(Optional) IP address or name of a multicast source.
<b>summary</b>	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
<b>count</b>	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
<b>active kbps</b>	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at a rate of <i>kbps</i> or higher. The <i>kbps</i> argument defaults to 4.

## show ip ospf database opaque-area

To display lists of information related to traffic engineering opaque link-state advertisements (LSAs), also known as Type-10 opaque link area link states, use the **show ip ospf database opaque-area** EXEC command.

```
show ip ospf database opaque-area
```

**Syntax Description** This command has no arguments or keywords.

## show ip ospf mpls traffic-eng

To display information about the links available on the local router for traffic engineering, use the **show ip ospf mpls traffic-eng** EXEC command.

```
show ip ospf [process-id [area-id]mpls traffic-eng [link] | [fragment]]
```

Syntax Description	
<b>process-id</b>	(Optional) Internal identification number that is assigned locally when the OSPF routing process is enabled. The value can be any positive integer.
<b>area-id</b>	(Optional) Area number associated with the OSPF
<b>link</b>	(Optional) Provides detailed information about the links over which traffic engineering is supported on the local router.
<b>fragment</b>	(Optional) Provides detailed information about the traffic engineering fragments on the local router.

## show ip pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** command in EXEC mode.

```
show ip pim interface [type number] [count]
```

### Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
<b>count</b>	(Optional) Number of packets received and sent out the interface.

## show ip protocols vrf

To display the routing protocol information associated with a VRF, use the **show ip protocols vrf** command in EXEC mode.

```
show ip protocols vrf vrf-name
```

### Syntax Description

<i>vrf-name</i>	Name assigned to a VRF.
-----------------	-------------------------

## show ip route vrf

To display the IP routing table associated with a VRF, use the **show ip route vrf** command in EXEC mode.

```
show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]] [list  
number [output-modifiers]] [profile] [static [output-modifiers]] [summary  
[output-modifiers]] [supernets-only [output-modifiers]] [traffic-engineering  
[output-modifiers]]
```

### Syntax Description

<i>vrf-name</i>	Name assigned to the VRF.
<b>connected</b>	(Optional) Displays all connected routes in a VRF.
<i>protocol</i>	(Optional) To specify a routing protocol, use one of the following keywords: <b>bgp</b> , <b>egp</b> , <b>eigrp</b> , <b>hello</b> , <b>igrp</b> , <b>isis</b> , <b>ospf</b> , or <b>rip</b> .
<i>as-number</i>	(Optional) Autonomous system number.
<i>tag</i>	(Optional) Cisco IOS routing area label.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<b>list number</b>	(Optional) Specifies the IP access list to display.
<b>profile</b>	(Optional) Displays the IP routing table profile.
<b>static</b>	(Optional) Displays static routes.
<b>summary</b>	(Optional) Displays a summary of routes.

<b>supernets-only</b>	(Optional) Displays supernet entries only.
<b>traffic-engineering</b>	(Optional) Displays only traffic-engineered routes.

## show ip rsvp host

To display RSVP terminal point information for receivers or senders, use the **show ip rsvp host EXEC** command.

```
show ip rsvp host {senders | receivers} [hostname | A.B.C.D]
```

Syntax Description		
<b>senders</b>	Displays information for senders.	
<b>receivers</b>	Displays information for receivers.	
<i>hostname</i>	(Optional) Restricts the display to sessions with <i>hostname</i> as their destination.	
<i>A.B.C.D</i>	(Optional) Restricts the display to sessions with the specified IP address as their destination.	

## show ip traffic-engineering

To display information about the traffic engineering configuration and metric information associated with it, use the **show ip traffic-engineering** command in privileged EXEC mode.

```
show ip traffic-engineering [metrics [detail]]
```

Syntax Description		
<b>metrics</b>	(Optional) Displays metric information associated with traffic engineering.	
<b>detail</b>	(Optional) Displays information in long form.	

## show ip traffic-engineering configuration

To display information about configured traffic engineering filters and routes, use the **show ip traffic-engineering configuration** privileged EXEC command.

```
show ip traffic-engineering configuration [interface] [filter-number] [detail]
```

Syntax Description		
<i>interface</i>	(Optional) Specifies an interface for which to display traffic engineering information.	
<i>filter-number</i>	(Optional) A decimal value representing the number of the filter to display.	
<b>detail</b>	(Optional) Displays command output in long form.	

## show ip traffic-engineering routes

To display information about the requested filters configured for traffic engineering, use the **show ip traffic-engineering routes** command in privileged EXEC mode.

```
show ip traffic-engineering routes [filter-number] [detail]
```

<b>Syntax Description</b>	<i>filter-number</i>	(Optional) A decimal value representing the number of the filter to display.
	<b>detail</b>	(Optional) Display of command output in long form.

## show ip vrf

To display the set of defined VRFs and associated interfaces, use the **show ip vrf** command in EXEC mode.

```
show ip vrf [{brief | detail | interfaces}] [vrf-name] [output-modifiers]
```

<b>Syntax Description</b>	<b>brief</b>	(Optional) Displays concise information on the VRFs and associated interfaces.
	<b>detail</b>	(Optional) Displays detailed information on the VRFs and associated interfaces.
	<b>interfaces</b>	(Optional) Displays detailed information about all interfaces bound to a particular VRF, or any VRF.
	<i>vrf-name</i>	(Optional) Name assigned to a VRF.
	<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

## show isis database verbose

To display additional information about the database, use the **show isis database verbose** EXEC command.

```
show isis database verbose
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## show isis mpls traffic-eng adjacency-log

To display a log of 20 entries of MPLS traffic engineering IS-IS adjacency changes, use the **show isis mpls traffic-eng adjacency-log** EXEC command.

```
show isis mpls traffic-eng adjacency-log
```

---

**Syntax Description** This command has no arguments or keywords.

## show isis mpls traffic-eng advertisements

To display the last flooded record from MPLS traffic engineering, use the **show isis mpls traffic-eng advertisements** EXEC command.

```
show isis mpls traffic-eng advertisements
```

---

**Syntax Description** This command has no arguments or keywords.

## show isis mpls traffic-eng tunnel

To display information about tunnels considered in the IS-IS next hop calculation, use the **show isis mpls traffic-eng tunnel** EXEC command.

```
show isis mpls traffic-eng tunnel
```

---

**Syntax Description** This command has no arguments or keywords.

## show lane

To display detailed information for all the LANE components configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane** command in EXEC mode.

**AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series**

```
show lane [interface atm slot/port[.subinterface-number] | name elan-name] [brief]
```

**ATM Port Adapter on the Cisco 7500 Series Routers**

```
show lane [interface atm slot/port-adapter/port[.subinterface-number] | name elan-name][brief]
```

**Cisco 4500 and 4700 Routers**

```
show lane [interface atm number[.subinterface-number] | name elan-name] [brief]
```

<b>Syntax Description</b>	<b>interface atm</b> <i>slot/port</i>	(Optional) ATM interface slot and port for the following: <ul style="list-style-type: none"> <li>• AIP on the Cisco 7500 series routers.</li> <li>• ATM port adapter on the Cisco 7200 series routers.</li> </ul>
	<b>interface atm</b> <i>slot/port-adapter/port</i>	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
	<b>interface atm</b> <i>number</i>	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
	<i>.subinterface-number</i>	(Optional) Subinterface number.
	<b>name</b> <i>elan-name</i>	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.
	<b>brief</b>	(Optional) Keyword used to display the brief subset of available information.

## show lane bus

To display detailed LANE information for the broadcast and unknown server (BUS) configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane bus** command in EXEC mode:

### AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

```
show lane bus [interface atm slot/port[.subinterface-number] | name elan-name] [brief]
```

### ATM Port Adapter on the Cisco 7500 Series Routers

```
show lane bus [interface atm slot/port-adapter/port[.subinterface-number] | name elan-name][brief]
```

### Cisco 4500 and 4700 Routers

```
show lane bus [interface atm number[.subinterface-number] | name elan-name] [brief]
```

<b>Syntax Description</b>	<b>interface atm</b> <i>slot/port</i>	(Optional) ATM interface slot and port for the following: <ul style="list-style-type: none"> <li>• AIP on the Cisco 7500 series routers.</li> <li>• ATM port adapter on the Cisco 7200 series routers.</li> </ul>
	<b>interface atm</b> <i>slot/port-adapter/port</i>	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
	<b>interface atm</b> <i>number</i>	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
	<i>.subinterface-number</i>	(Optional) Subinterface number.

<b>name</b> <i>elan-name</i>	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.
<b>brief</b>	(Optional) Displays the brief subset of available information.

## show lane client

To display detailed LANE information for all the LANE clients configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane client** command in EXEC mode.

### AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

```
show lane client detail [interface atm slot/port[.subinterface-number] | name elan-name] [brief]
```

### ATM Port Adapter on the Cisco 7500 Series Routers

```
show lane client detail [interface atm slot/port-adapter/port[.subinterface-number] | name elan-name] [brief]
```

### Cisco 4500 and 4700 Routers

```
show lane client detail [interface atm number[.subinterface-number] | name elan-name] [brief]
```

#### Syntax Description

<b>detail</b>	Displays additional FSSRP information.
<b>interface atm</b> <i>slot/port</i>	(Optional) ATM interface slot and port for the following: <ul style="list-style-type: none"> <li>AIP on the Cisco 7500 series routers.</li> <li>ATM port adapter on the Cisco 7200 series routers.</li> </ul>
<b>interface atm</b> <i>slot/port-adapter/port</i>	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
<b>interface atm</b> <i>number</i>	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
<i>.subinterface-number</i>	(Optional) Subinterface number.
<b>name</b> <i>elan-name</i>	(Optional) Name of ELAN. The maximum length of the name is 32 characters.
<b>brief</b>	(Optional) Displays the brief subset of available information.

## show lane config

To display global LANE information for the configuration server configured on an interface, use the **show lane config** command in EXEC mode.

### AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

```
show lane config [interface atm slot/0]
```

### ATM Port Adapter on the Cisco 7500 Series Routers

```
show lane config [interface atm slot/port-adapter/0]
```

### Cisco 4500 and 4700 Routers

```
show lane config [interface atm number]
```

Syntax Description		
<b>interface atm slot/0</b>	(Optional) ATM interface slot and port for the following:	<ul style="list-style-type: none"> <li>• AIP on the Cisco 7500 series routers.</li> <li>• ATM port adapter on the Cisco 7200 series routers.</li> </ul>
<b>interface atm slot/port-adapter/0</b>	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.	
<b>interface atm number</b>	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.	

## show lane database

To display the database of the configuration server, use the **show lane database** command in EXEC mode.

```
show lane database [database-name]
```

Syntax Description	<i>database-name</i>	(Optional) Specific database name.

## show lane default-atm-addresses

To display the automatically assigned ATM address of each LANE component in a router or on a specified interface or subinterface, use the **show lane default-atm-addresses** command in EXEC mode.

### AIP on the Cisco 7500 series routers; ATM port adapter on the Cisco 7200 series

```
show lane default-atm-addresses [interface atm slot/port.subinterface-number]
```

**ATM Port Adapter on the Cisco 7500 Series Routers**

```
show lane default-atm-addresses [interface atm slot/port-adapter/port.subinterface-number]
```

**Cisco 4500 and 4700 Routers**

```
show lane default-atm-addresses [interface atm number.subinterface-number]
```

**Syntax Description**

<b>interface atm</b> <i>slot/port</i>	(Optional) ATM interface slot and port for the following: <ul style="list-style-type: none"> <li>• AIP on the Cisco 7500 series routers.</li> <li>• ATM port adapter on the Cisco 7200 series routers.</li> </ul>
<b>interface atm</b> <i>slot/port-adapter/port</i>	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
<b>interface atm</b> <i>number</i>	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
<i>.subinterface-number</i>	(Optional) Subinterface number.

## show lane le-arp

To display the LANE ARP table of the LANE client configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane le-arp** command in EXEC mode.

**AIP on the Cisco 7500 series routers; ATM Port Adapter on the Cisco 7200 series**

```
show lane le-arp [interface atm slot/port[.subinterface-number] | name elan-name]
```

**ATM Port Adapter on the Cisco 7500 Series Routers**

```
show lane le-arp [interface atm slot/port-adapter/port[.subinterface-number] | name elan-name]
```

**Cisco 4500 and 4700 Routers**

```
show lane le-arp [interface atm number[.subinterface-number] | name elan-name]
```

**Syntax Description**

<b>interface atm</b> <i>slot/port</i>	(Optional) ATM interface slot and port for the following: <ul style="list-style-type: none"> <li>• AIP on the Cisco 7500 series routers.</li> <li>• ATM port adapter on the Cisco 7200 series routers.</li> </ul>
<b>interface atm</b> <i>slot/port-adapter/port</i>	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.

<b>interface atm</b> <i>number</i>	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
<i>.subinterface-number</i>	(Optional) Subinterface number.
<b>name</b> <i>elan-name</i>	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.

## show lane server

To display global information for the LANE server configured on an interface, on any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane server** command in EXEC mode.

### AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

```
show lane server [interface atm slot/port[.subinterface-number] | name elan-name] [brief]
```

### ATM Port Adapter on the Cisco 7500 Series Routers

```
show lane server [interface atm slot/port-adapter/port[.subinterface-number] | name elan-name] [brief]
```

### Cisco 4500 and 4700 Routers

```
show lane server [interface atm number[.subinterface-number] | name elan-name] [brief]
```

### Syntax Description

<b>interface atm</b> <i>slot/port</i>	(Optional) ATM interface slot and port for the following: <ul style="list-style-type: none"> <li>• AIP on the Cisco 7500 series routers.</li> <li>• ATM port adapter on the Cisco 7200 series routers.</li> </ul>
<b>interface atm</b> <i>slot/port-adapter/port</i>	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
<b>interface atm</b> <i>number</i>	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
<i>.subinterface-number</i>	(Optional) Subinterface number.
<b>name</b> <i>elan-name</i>	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.
<b>brief</b>	(Optional) Keyword used to display the brief subset of available information.

## show mls rp

To display MLS details, including specifics for MLSP, use the **show mls rp** command in EXEC mode.

```
show mls rp [interface]
```

<b>Syntax Description</b>	<i>interface</i>	(Optional) Displays information for one interface. Without this argument, detailed views of all interfaces are displayed.
---------------------------	------------------	---

## show mls rp interface

To display IPX Multilayer Switching (MLS) details for the Route Processor (RP), including specific information about the Multilayer Switching Protocol (MLSP), use the **show mls rp interface** command in privileged EXEC mode.

```
show mls rp interface type number
```

<b>Syntax Description</b>	<i>type</i>	Interface type.
	<i>number</i>	Interface number.

## show mls rp ip multicast

To display hardware-switched multicast flow information about IP multicast Multilayer Switching (MLS), use the **show mls rp ip multicast** command in EXEC mode.

```
show mls rp ip multicast [locate] [group [source] [vlan-id ]] | [statistics] | [summary]
```

<b>Syntax Description</b>	<b>locate</b>	(Optional) Displays flow information associated with the switch. This keyword applies only to a single router and multiple switches.
	<i>group</i>	(Optional) Address of the IP multicast group about which to display information.
	<i>source</i>	(Optional) IP multicast source sending to the specified multicast <i>group</i> about which to display information.
	<i>vlan-id</i>	(Optional) Source VLAN about which to display information.
	<b>statistics</b>	(Optional) Displays MLS statistics.
	<b>summary</b>	(Optional) Displays MLS summary.

## show mls rp ipx

To display details for all IPX Multilayer Switching (MLS) interfaces on the IPX MLS router, use the **show mls rp ipx** command in privileged EXEC mode.

```
show mls rp ipx
```

---

**Syntax Description** This command has no arguments or keywords.

## show mls rp vtp-domain

To display IPX Multilayer Switching (MLS) interfaces for a specific Virtual Trunk Protocol (VTP) domain on the Route Processor (RP), use the **show mls rp vtp-domain** command in privileged EXEC mode.

```
show mls rp vtp-domain domain-name
```

---

**Syntax Description**

<i>domain-name</i>	The name of the VTP domain whose MLS interfaces will be displayed.
--------------------	--

---

## show mpls forwarding-table

To display the contents of the MPLS forwarding information base (LFIB), use the **show mpls forwarding-table** user EXEC command.

```
show mpls forwarding-table [{network {mask | length} | labels label [- label] | interface interface | next-hop address | lsp-tunnel [tunnel-id ]}] [detail]
```

---

**Syntax Description**

<i>network</i>	(Optional) Destination network number.
<i>mask</i>	(Optional) IP address of the destination mask whose entry is to be shown.
<i>length</i>	(Optional) Number of bits in mask of destination.
<b>labels</b> <i>label - label</i>	(Optional) Displays only entries with the specified local labels.
<b>interface</b> <i>interface</i>	(Optional) Displays only entries with the specified outgoing interface.
<b>next-hop</b> <i>address</i>	(Optional) Displays only entries with the specified neighbor as the next hop.
<b>lsp-tunnel</b> <i>tunnel-id</i>	(Optional) Displays only entries with the specified LSP tunnel, or all LSP tunnel entries.
<b>detail</b>	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit (MTU), and all labels).

---

## show mpls interfaces

To display information about one or more interfaces that have been configured for label switching, use the **show mpls interfaces** privileged EXEC command.

```
show mpls interfaces [interface] [detail]
```

```
show mpls interfaces [all]
```

Syntax Description		
	<i>interface</i>	(Optional) Defines the interface about which to display label switching information.
	<b>detail</b>	(Optional) Displays detailed label switching information for the specified interface.
	<b>all</b>	(Optional) When the <b>all</b> keyword is specified in the absence of other optional parameters, the command displays LDP discovery information for all VPNs.

## show mpls label range

To display the range of local labels available for use on packet interfaces, use the **show mpls label range** privileged EXEC command.

```
show mpls label range
```

**Syntax Description** This command has no optional keywords or arguments

## show mpls traffic-eng autoroute

To show tunnels that are announced to the Interior Gateway Protocol (IGP), including interface, destination, and bandwidth, use the **show mpls traffic-eng autoroute** EXEC command.

```
show mpls traffic-eng autoroute
```

**Syntax Description** This command has no arguments or keywords.

## show mpls traffic-eng link-management admission-control

To show which tunnels were admitted locally and their parameters (such as, priority, bandwidth, incoming and outgoing interface, and state), use the **show mpls traffic-eng link-management admission-control** EXEC command.

```
show mpls traffic-eng link-management admission-control [interface-name]
```

<b>Syntax Description</b>	<i>interface-name</i>	(Optional) Displays only tunnels that were admitted on the specified interface.
---------------------------	-----------------------	---

## show mpls traffic-eng link-management advertisements

To show local link information that MPLS traffic engineering link management is currently flooding into the global traffic engineering topology, use the **show mpls traffic-eng link-management advertisements** EXEC command.

```
show mpls traffic-eng link-management advertisements
```

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## show mpls traffic-eng link-management bandwidth-allocation

To show current local link information, use the **show mpls traffic-eng link-management bandwidth-allocation** EXEC command.

```
show mpls traffic-eng link-management bandwidth-allocation [interface-name]
```

<b>Syntax Description</b>	<i>interface-name</i>	(Optional) Displays only tunnels that were admitted on the specified interface.
---------------------------	-----------------------	---

## show mpls traffic-eng link-management igp-neighbors

To show Interior Gateway Protocol (IGP) neighbors, use the **show mpls traffic-eng link-management igp-neighbors** EXEC command.

```
show mpls traffic-eng link-management igp-neighbors [{igp-id {isis isis-address |  
ospf ospf-id} | ip A.B.C.D}]
```

<b>Syntax Description</b>	<i>igp-id</i>	(Optional) Displays the IGP neighbors that are using a specified IGP identification.
	<b>isis</b> <i>isis-address</i>	(Optional) Displays the specified IS-IS neighbor when you display neighbors by IGP ID.
	<b>ospf</b> <i>ospf-id</i>	(Optional) Displays the specified OSPF neighbor when you display neighbors by IGP ID.
	<b>ip</b> <i>A.B.C.D</i>	(Optional) Displays the IGP neighbors that are using a specified IGP IP address.

## show mpls traffic-eng link-management interfaces

To show interface resource and configuration information, use the **show mpls traffic-eng link-management interfaces EXEC** command.

```
show mpls traffic-eng link-management interfaces [interface-name]
```

<b>Syntax Description</b>	<i>interface-name</i>	(Optional) Displays information only for the specified interface.
---------------------------	-----------------------	---

## show mpls traffic-eng link-management summary

To show a summary of link management information, use the **show mpls traffic-eng link-management summary EXEC** command.

```
show mpls traffic-eng link-management summary [interface-name]
```

<b>Syntax Description</b>	<i>interface-name</i>	(Optional) Displays information only for the specified interface.
---------------------------	-----------------------	---

## show mpls traffic-eng topology

To show the MPLS traffic engineering global topology currently known at this node, use the **show mpls traffic-eng topology EXEC** command.

```
show mpls traffic-eng topology [{A.B.C.D | igp-id {isis nsapaddr | ospf A.B.C.D}}] [brief]
```

<b>Syntax Description</b>	<i>A.B.C.D</i>	(Optional) Node IP address (router identifier to interface address).
	<b>igp-id</b>	(Optional) Node IGP router identifier.
	<b>isis</b> <i>nsapaddr</i>	(Optional) Node router identification, if IS-IS is enabled.
	<b>ospf</b> <i>A.B.C.D</i>	(Optional) Node router identifier, if OSPF is enabled.
	<b>brief</b>	(Optional) Brief form of the output; gives a less detailed version of the topology.

## show mpls traffic-eng topology path

To show the properties of the best available path to a specified destination that satisfies certain constraints, use the **show mpls traffic-eng topology path EXEC** command.

```
show mpls traffic-eng topology path {tunnel-interface [destination address]
| destination address}[bandwidth value] [priority value [value]]
affinity value [mask mask]]
```

Syntax Description		
<i>tunnel-interface</i>	Name of an MPLS traffic engineering interface (for example, Tunnel1) from which default constraints should be copied.	
<b>destination</b> <i>address</i>	(Optional) IP address specifying the path's destination.	
<b>bandwidth</b> <i>value</i>	(Optional) Bandwidth constraint. The amount of available bandwidth that a suitable path requires. This overrides the bandwidth constraint obtained from the specified tunnel interface. You can specify any positive number.	
<b>priority</b> <i>value</i> [ <i>value</i> ]	(Optional) Priority constraints. The setup and hold priorities used to acquire bandwidth along the path. If specified, this overrides the priority constraints obtained from the tunnel interface. Valid values are from 0 to 7.	
<b>affinity</b> <i>value</i>	(Optional) Affinity constraints. The link attributes for which the path has an affinity. If specified, this overrides the affinity constraints obtained from the tunnel interface.	
<b>mask</b> <i>mask</i>	(Optional) Affinity constraints. The mask associated with the affinity specification.	

## show mpls traffic-eng tunnels

To show information about tunnels, use the **show mpls traffic-eng tunnels EXEC** command.

```
show mpls traffic-eng tunnels tunnel-interface [brief]
```

```
show mpls traffic-eng tunnels
[destination address]
[source-id {num | ipaddress | ipaddress num}]
[role {all | head | middle | tail | remote}]
[up | down]
[name string]
[suboptimal constraints {none | current | max}]
[interface in phys-intf] [interface out phys-intf] | [interface phys-intf]]
[brief]
```

Syntax Description		
<i>tunnel-interface</i>	Displays information for the specified tunneling interface.	
<b>brief</b>	(Optional) Displays the information in brief format.	
<b>destination</b> <i>address</i>	(Optional) Restricts the display to tunnels destined to the specified IP address.	
<b>source-id</b>	(Optional) Restricts the display to tunnels with a matching source IP address or tunnel number.	

<i>num</i>	(Optional) Tunnel number.
<i>ipaddress</i>	(Optional) Source IP address.
<i>ipaddress num</i>	(Optional) Source IP address and tunnel number.
<b>role</b>	(Optional) Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
<b>all</b>	(Optional) Displays all tunnels.
<b>head</b>	(Optional) Displays tunnels with their heads at this router.
<b>middle</b>	(Optional) Displays tunnels with their midpoints at this router.
<b>tail</b>	(Optional) Displays tunnels with their tails at this router.
<b>remote</b>	(Optional) Displays tunnels with their heads at another router; this is a combination of the <b>middle</b> and <b>tail</b> keyword values.
<b>up</b>	(Optional) Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
<b>down</b>	(Optional) Displays tunnels that are down.
<b>name</b> <i>string</i>	(Optional) Displays tunnels with the specified name. The tunnel name is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel name is included in the signalling message so it is available at all hops.
<b>suboptimal constraints none</b>	(Optional) Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the IGP's shortest path.
<b>suboptimal constraints current</b>	(Optional) Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options. Selected tunnels would have a shorter path if they were reoptimized immediately.
<b>suboptimal constraints max</b>	(Optional) Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options, and considering only the network's capacity. Selected tunnels would have a shorter path if no other tunnels were consuming network resources.
<b>interface in</b> <i>phys-intf</i>	(Optional) Displays tunnels that use the specified input interface.
<b>interface out</b> <i>phys-intf</i>	(Optional) Displays tunnels that use the specified output interface.
<b>interface</b> <i>phys-intf</i>	(Optional) Displays tunnels that use the specified interface as an input or output interface.
<b>brief</b>	(Optional) Specifies one line per tunnel.

## show mpls traffic-eng tunnels summary

To show summary information about tunnels, use the **show mpls traffic-eng tunnels summary EXEC** command.

**show mpls traffic-eng tunnels summary**

### Syntax Description

This command has no arguments or keywords.

## show mpoa client

To display a summary of information regarding one or all MPCs, use the **show mpoa client** command in EXEC mode.

```
show mpoa client [name mpc-name] [brief]
```

---

### Syntax Description

<b>name</b> <i>mpc-name</i>	(Optional) Name of the MPC with the specified name.
<b>brief</b>	(Optional) Output limit of the command.

---

## show mpoa client cache

To display the ingress or egress cache entries matching the IP addresses for the MPCs, use the **show mpoa client cache** command in EXEC mode.

```
show mpoa client [name mpc-name] cache [ingress | egress] [ip-address ip-address]
```

---

### Syntax Description

<b>name</b> <i>mpc-name</i>	(Optional) Name of the MPC with the specified name.
<b>ingress</b>	(Optional) Displays ingress cache entries associated with an MPC.
<b>egress</b>	(Optional) Displays egress cache entries associated with an MPC.
<b>ip-address</b> <i>ip-address</i>	(Optional) Displays cache entries that match the specified IP address.

---

## show mpoa client statistics

To display all the statistics collected by an MPC, use the **show mpoa client statistics** command in EXEC mode.

```
show mpoa client [name mpc-name] statistics
```

---

### Syntax Description

<b>name</b> <i>mpc-name</i>	(Optional) Specifies the name of the MPC.
-----------------------------	---

---

## show mpoa default-atm-addresses

To display the default ATM addresses for the MPC, use the **show mpoa default-atm-addresses** command in EXEC mode.

```
show mpoa default-atm-addresses
```

---

### Syntax Description

This command has no arguments or keywords.

## show mpoa server

To display information about any specified MPS or all MPSs in the system, depending on whether the name of the required MPS is specified, use the **show mpoa server** command in EXEC mode.

```
show mpoa server [name mps-name]
```

Syntax Description	name <i>mps-name</i>	(Optional) Specifies the name of the MPOA server.
--------------------	----------------------	---

## show mpoa server cache

To display ingress and egress cache entries associated with an MPS, use the **show mpoa server cache** command in EXEC mode.

```
show mpoa server [name mps-name] cache [ingress | egress] [ip-address ip-address]
```

Syntax Description	name <i>mps-name</i>	(Optional) Specifies the name of an MPOA server.
	ingress	(Optional) Displays ingress cache entries associated with a server.
	egress	(Optional) Displays egress cache entries associated with a server.
	ip-address <i>ip-address</i>	(Optional) Displays the entries that match the specified IP address.

## show mpoa server statistics

To display all the statistics collected by an MPS, use the **show mpoa server statistics** command in EXEC mode.

```
show mpoa server [name mps-name] statistics
```

Syntax Description	name <i>mps-name</i>	(Optional) Specifies the name of an MPOA server.
--------------------	----------------------	--

## show pxf accounting

To show PXF switching statistics for individual interfaces, use the **show pxf accounting** EXEC command.

```
show pxf accounting interface [slot/port]
```

Syntax Description	interface	Specifies the type of interface to display.
	slot	(Optional) Backplane slot number. On the Cisco 7200 VXR series routers, the value can be from 0 to 6.
	port	(Optional) Port number of the interface. On the Cisco 7200 VXR series routers, the value can be from 0 to 5.

## show pxf crash

To show PXF crash information, use the **show pxf crash** EXEC command.

```
show pxf crash
```

---

**Syntax Description** This command has no arguments or keywords.

## show pxf feature cef

To display PXF routing feature tables for Cisco Express Forwarding (CEF), use the **show pxf feature cef** EXEC command.

```
show pxf feature cef entry
```

---

**Syntax Description**

<i>entry</i>	Display the PXF entry.
--------------	------------------------

---

## show pxf feature nat

To display PXF routing tables for Network Address Translation (NAT), use the **show pxf feature nat** EXEC command.

```
show pxf feature nat [entry | stat | tcp]
```

---

**Syntax Description**

<i>entry</i>	Displays NAT information.
<i>stat</i>	Displays NAT processing information.
<i>tcp</i>	Displays NAT TCP logging information.

---

## show pxf interface

To show a summary of the interfaces on the router and the PXF features or capabilities enabled on these interfaces, use the **show pxf interface** command.

```
show pxf interface
```

---

**Syntax Description** This command has no arguments or keywords.

## show route-map ipc

To display counts of the one-way route map IPC messages sent from the RP to the VIP when NetFlow policy routing is configured, use the **show route-map ipc** command in EXEC mode.

```
show route-map ipc
```

**Syntax Description** This command has no arguments or keywords.

## show tag-switching atm-tdp bindings

To display the requested entries from the ATM LDP label bindings database, use the **show tag-switching atm-tdp bindings** EXEC command.

```
show tag-switching atm-tdp bindings [A.B.C.D {mask | length}][local-tag | remote-tag vpi vci]
[neighbor atm slot/subslot/port][remote-tag vpi vci]
```

<b>Syntax Description</b>	<i>A.B.C.D</i>	(Optional) Destination of the prefix.
	<i>mask</i>	(Optional) Destination netmask prefix.
	<i>length</i>	(Optional) Netmask length, in the range from 1 to 32.
	<b>local-tag</b> <i>vpi vci</i>	(Optional) Matches locally assigned label values.
	<b>neighbor atm</b> <i>slot/subslot/port</i>	(Optional) Matches labels assigned by a neighbor on the specified ATM interface.
	<b>remote-tag</b> <i>vpi vci</i>	(Optional) Matches remotely assigned label values.

## show tag-switching atm-tdp bindwait

To display the number of bindings waiting for label assignments from a remote MPLS ATM switch, use the **show tag-switching atm-tdp bindwait** EXEC command.

```
show tag-switching atm-tdp bindwait
```

**Syntax Description** This command has no keywords or arguments.

## show tag-switching atm-tdp capability

To display the ATM LDP label capabilities, use the **show tag-switching atm-tdp capability** command in privileged EXEC mode.

```
show tag-switching atm-tdp capability
```

**Syntax Description** This command has no arguments or keywords.

## show tag-switching atm-tdp summary

To display summary information on ATM label bindings, use the **show tag-switching atm-tdp summary** command in privileged EXEC mode.

```
show tag-switching atm-tdp summary
```

---

**Syntax Description** This command has no arguments or keywords.

## show tag-switching cos-map

To display the QoS map used to assign a quantity of label VCs (LVCs) and an associated QoS of those LVCs, use the **show tag-switching cos-map** EXEC command in EXEC mode.

```
show tag-switching cos-map
```

---

**Syntax Description** This command has no arguments or keywords.

## show tag-switching forwarding-table

To display the contents of the Label Forwarding Information Base (LFIB), use the **show tag-switching forwarding-table** command in privileged EXEC mode.

```
show tag-switching forwarding-table [{network {mask | length} | tags tag [- tag] | interface
interface | next-hop address | tsp-tunnel [tunnel-id ]}] [detail]
```

---

<b>Syntax Description</b>	<i>network</i>	(Optional) Destination network number.
	<i>mask</i>	(Optional) IP address of the destination mask whose entry is to be shown.
	<i>length</i>	(Optional) Number of bits in the mask of destination.
	<b>tags tag - tag</b>	(Optional) Displays entries with the specified local labels only.
	<b>interface interface</b>	(Optional) Displays entries with the specified outgoing interface only.
	<b>next-hop address</b>	(Optional) Displays entries with the specified neighbor as next hop only.
	<b>tsp-tunnel [tunnel-id]</b>	(Optional) Displays entries with the specified LSP tunnel only, or all LSP tunnel entries.
	<b>detail</b>	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit (MTU), and all labels).

---

## show tag-switching forwarding vrf

To display label forwarding information for advertised VRF routes, use the **show tag-switching forwarding vrf** command in EXEC mode. To disable the display of label forwarding information, use the **no** form of this command.

```
show tag-switching forwarding vrf vrf-name [ip-prefix/length [mask]] [detail] [output-modifiers]
```

```
no show tag-switching forwarding vrf vrf-name [ip-prefix/length [mask]] [detail]
[output-modifiers]
```

Syntax Description		
	<i>vrf-name</i>	Displays NLRIs associated with the named VRF.
	<i>ip-prefix/length</i>	(Optional) IP prefix address (in dotted decimal format) and length of mask (0 to 32).
	<i>mask</i>	(Optional) Destination network mask, in dotted decimal format.
	<b>detail</b>	(Optional) Displays detailed information on the VRF routes.
	<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use the Cisco IOS command-line interface (CLI).

## show tag-switching interfaces

To display information about one or more interfaces that have the MPLS feature enabled, use the **show tag-switching interfaces** command in EXEC mode.

```
show tag-switching interfaces [interface] [detail]
```

Syntax Description		
	<i>interface</i>	(Optional) The interface about which to display MPLS information.
	<b>detail</b>	(Optional) Displays information in long form.

## show tag-switching prefix-map

To show the prefix map used to assign a QoS map to network prefixes matching a standard IP access list, use the **show tag-switching prefix-map** command in EXEC mode.

```
show tag-switching prefix-map [prefix-map]
```

Syntax Description		
	<i>prefix-map</i>	(Optional) Specifies the prefix-map number.

## show tag-switching tdp bindings

To display the contents of the label information base (LIB), use the **show tag-switching tdp bindings** command in privileged EXEC mode.

```
show tag-switching tdp bindings [network{mask | length} [longer-prefixes]] [local-tag tag
[- tag]] [remote-tag tag [- tag]] [neighbor address] [local]
```

Syntax Description		
	<i>network</i>	(Optional) Destination network number.
	<i>mask</i>	(Optional) Network mask written as A.B.C.D.
	<i>length</i>	(Optional) Mask length (1 to 32 characters).
	<b>longer-prefixes</b>	(Optional) Selects any prefix that matches the <i>mask</i> with <i>length</i> value to 32.
	<b>local-tag</b> <i>tag - tag</i>	(Optional) Displays entries matching local label values by this router. Use the <i>- tag</i> argument to indicate the label range.
	<b>remote-tag</b> <i>tag - tag</i>	(Optional) Displays entries matching label values assigned by a neighbor router. Use the <i>- tag</i> argument to indicate the label range.
	<b>neighbor</b> <i>address</i>	(Optional) Displays label bindings assigned by selected neighbor.
	<b>local</b>	(Optional) Displays local label bindings.

## show tag-switching tdp discovery

To display the status of the LDP discovery process, use the **show tag-switching tdp discovery** command in privileged EXEC mode.

**Syntax Description** This command has no arguments or keywords.

## show tag-switching tdp neighbors

To display the status of Label Distribution Protocol (LDP) sessions, use the **show tag-switching tdp neighbors** command in privileged EXEC mode.

```
show tag-switching tdp neighbors [address | interface] [detail]
```

Syntax Description		
	<i>address</i>	(Optional) The neighbor that has this IP address.
	<i>interface</i>	(Optional) LDP neighbors accessible over this interface.
	<b>detail</b>	(Optional) Displays information in long form.

## show tag-switching tdp parameters

To display available LDP (TDP) parameters, use the **show tag-switching tdp parameters** command in privileged EXEC mode.

```
show tag-switching tdp parameters
```

**Syntax Description** This command has no arguments or keywords.

## show tag-switching tsp-tunnels

To display information about the configuration and status of selected tunnels, use the **show tag-switching tsp-tunnels** command in privileged EXEC mode.

```
show tag-switching tsp-tunnels [{head | middle | tail | all | remote | address}
[interface-number]] [brief]
```

<b>Syntax Description</b>	<b>head</b>	(Optional) Displays information for tunnels that originate at the node.
	<b>middle</b>	(Optional) Displays information for tunnels that pass through the node.
	<b>tail</b>	(Optional) Displays information for tunnels that terminate at the node.
	<b>all</b>	(Optional) Displays the combination of head, middle, and tail information for tunnels.
	<b>remote</b>	(Optional) Displays information for tunnels that originate elsewhere; it is thus the combination of middle and tail information.
	<i>address</i>	(Optional) Displays information for tunnels that use the specified address in their identifier.
	<i>interface-number</i>	(Optional) Displays information for tunnels that use the specified number in their identifier.
	<b>brief</b>	(Optional) Displays a brief summary of tunnel status and configuration.

## show vlans

To view virtual LAN (VLAN) subinterfaces, use the **show vlans** privileged EXEC command.

```
show vlans
```

**Syntax Description** This command has no arguments or keywords.

## show xtagatm cos-bandwidth-allocation XTagATM

To display information about QoS bandwidth allocation on extended MPLS ATM interfaces, use the **show xtagatm cos-bandwidth-allocation XTagATM EXEC** command.

```
show xtagatm cos-bandwidth-allocation XTagATM [XTagATM interface number]
```

---

### Syntax Description

<b>XTagATM interface number</b>	(Optional) Specifies the XTagATM interface number.
---------------------------------	--

---

## show xtagatm cross-connect

To display information about the LSC view of the cross-connect table on the remotely controlled ATM switch, use the **show xtagatm cross-connect EXEC** command.

```
show xtagatm cross-connect [traffic] [{interface interface [vpi vci] | descriptor descriptor [vpi vci]]
```

---

### Syntax Description

<b>traffic</b>	(Optional) Displays receive and transmit cell counts for each connection.
<b>interface interface</b>	(Optional) Displays only connections with an endpoint of the specified interface.
<b>vpi vci</b>	(Optional) Displays only detailed information on the endpoint with the specified VPI/VCI on the specified interface.
<b>descriptor descriptor</b>	(Optional) Displays only connections with an endpoint on the interface with the specified physical descriptor.

---

## show xtagatm vc

To display information about terminating VCs on extended MPLS ATM (XTagATM) interfaces, use the **show xtagatm vc EXEC** command.

```
show xtagatm vc [vcd [interface]]
```

---

### Syntax Description

<b>vcd</b>	(Optional) Virtual circuit descriptor (virtual circuit number). If you specify the <i>vcd</i> argument, then detailed information about all VCs with that <i>vcd</i> appears. If you do not specify the <i>vcd</i> argument, a summary description of all VCs on all XTagATM interfaces appears.
<b>interface</b>	(Optional) Interface number. If you specify the <i>interface</i> and the <i>vcd</i> arguments, the single VC with the specified <i>vcd</i> on the specified <i>interface</i> is selected.

---

## tag-control-protocol vsi

To configure the use of VSI on a particular master control port, use the **tag-control-protocol vsi** interface configuration command. To disable VSI, use the **no** form of this command.

```
tag-control-protocol vsi [id controller-id] [base-vc vpi vci] [slaves slave-count]
[keepalive timeout] [retry timeout-count]
```

```
no tag-control-protocol vsi [id controller-id] [base-vc vpi vci] [slaves slave-count]
[keepalive timeout] [retry timeout-count]
```

Syntax Description	
<b>id</b> <i>controller-id</i>	(Optional) Determines the value of the controller-id field present in the header of each VSI message. The default is 1.
<b>base-vc</b> <i>vpi vci</i>	(Optional) Determines the VPI/VCI value for the channel to the first slave. The default is 0/40.  Together with the slave value, this value determines the VPI/VCI values for the channels to all of the slaves, which are as follows: <ul style="list-style-type: none"> <li>• <i>vpi/vci</i></li> <li>• <i>vpi/vci+1</i>, and so on</li> <li>• <i>vpi/vci+slave_count-1</i></li> </ul>
<b>slaves</b> <i>slave-count</i>	(Optional) Determines the number of slaves reachable through this master control port. The default is 14 (suitable for the Cisco BPX switch).
<b>keepalive</b> <i>timeout</i>	(Optional) Determines the value of the keepalive timer (in seconds). Make sure that the keepalive timer value is greater than the value of the <i>retry_timer</i> times the <i>retry_count+1</i> . The default is 15 seconds.
<b>retry</b> <i>timeout-count</i>	(Optional) Determines the value of the message retry timer (in seconds) and the maximum number of retries. The default is 8 seconds and 10 retries.

## tag-switching advertise-tags

To control the distribution of locally assigned (incoming) labels via the Label Distribution Protocol (LDP), use the **tag-switching advertise-tags** command in global configuration mode. To disable label advertisement, use the **no** form of this command.

```
tag-switching advertise-tags [for access-list-number [to access-list-number]]
```

```
no tag-switching advertise-tags [for access-list-number [to access-list-number]]
```

Syntax Description	
<b>for</b> <i>access-list-number</i>	(Optional) Specifies which destinations should have their labels advertised.
<b>to</b> <i>access-list-number</i>	(Optional) Specifies which LSR neighbors should receive label advertisements.  An LSR is identified by the router ID that is the first 4 bytes of its 6-byte LDP identifier.

## tag-switching atm allocation-mode

To control the mode used for handling label binding requests on TC-ATM interfaces, use the **tag-switching atm allocation-mode** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
tag-switching atm allocation-mode { optimistic | conservative }
```

```
no tag-switching atm allocation-mode { optimistic | conservative }
```

### Syntax Description

<b>optimistic</b>	Label binding is returned immediately, and packets are discarded until the downstream setup is complete.
<b>conservative</b>	Label binding is delayed until the label VC has been set up downstream.

## tag-switching atm control-vc

To configure the VPI and VCI values to be used for the initial link to the MPLS peer, use the **tag-switching atm control-vc** interface configuration command. To disable this feature, use the **no** form of this command.

```
tag-switching atm control-vc vpi vci
```

```
no tag-switching atm control-vc vpi vci
```

### Syntax Description

<i>vpi</i>	Virtual path identifier, in the range from 0 to 255.
<i>vci</i>	Virtual circuit identifier, in the range from 1 to 65535.

## tag-switching atm cos

To change the value of configured bandwidth allocation for QoS, use the **tag-switching atm cos** global configuration command.

```
tag-switching atm cos [available | standard | premium | control] weight
```

### Syntax Description

<b>available</b>	(Optional) Specifies the weight for the <b>available</b> class. This is the lowest class priority.
<b>standard</b>	(Optional) Specifies the weight for the <b>standard</b> class. This is the next lowest class priority.
<b>premium</b>	(Optional) Specifies the weight for the <b>premium</b> class. This is the next highest class priority.
<b>control</b>	(Optional) Specifies the weight for the <b>control</b> class. This is the highest class priority.
<i>weight</i>	Specifies the total weight for all QoS traffic classes. This value ranges from 0 to 100.

## tag-switching atm disable-headend-vc

To remove all headend VCs from the MPLS LSC and disable its ability to function as an edge LSR, use the **tag-switching atm disable-headend-vc** command. To restore the headend VCs of the MPLS LSC and restores full edge LSR functionality, use the **no** form of this command.

```
tag-switching atm disable-headend-vc
```

```
no tag-switching atm disable-headend-vc
```

---

**Syntax Description** This command has no arguments or keywords.

## tag-switching atm maxhops

To limit the maximum hop count to a value you have specified, use the **tag-switching atm maxhops** command in global configuration mode. To ignore the hop count, use the **no** form of this command.

```
tag-switching atm maxhops [number]
```

```
no tag-switching atm maxhops
```

---

**Syntax Description** *number* (Optional) Maximum hop count.

---

## tag-switching atm multi-vc

To configure a router subinterface to create one or more tag-VCs over which packets of different classes are sent, use the **tag-switching atm multi-vc** command in ATM subinterface configuration submode. To disable this option, use the **no** form of this command.

```
tag-switching atm multi-vc
```

```
no tag-switching atm multi-vc
```

---

**Syntax Description** This command has no arguments or keywords.

## tag-switching atm vc-merge

To control whether vc-merge (multipoint-to-point) is supported for unicast label VCs, use the **tag-switching atm vc-merge** command in global configuration mode. To disable this feature, use the **no** form of this command.

**tag-switching atm vc-merge**

**no tag-switching atm vc-merge**

---

**Syntax Description** This command has no arguments or keywords.

## tag-switching atm vpi

To configure the range of values to use in the VPI field for label VCs, use the **tag-switching atm vpi** interface configuration command. To clear the interface configuration, use the **no** form of this command.

**tag-switching atm vpi** *vpi* [- *vpi*]

**no tag-switching atm vpi** *vpi* [- *vpi*]

---

<b>Syntax Description</b>	<i>vpi</i>	Virtual path identifier, low end of range (from 1 to 255).
	- <i>vpi</i>	(Optional) Virtual path identifier, high end of range (from 1 to 255).

---

## tag-switching atm vp-tunnel

To specify an interface or a subinterface as a VP tunnel, use the **tag-switching atm vp-tunnel** interface configuration command.

**tag-switching atm vp-tunnel** *vpi*

---

<b>Syntax Description</b>	<i>vpi</i>	Provides VPI value for the local end of the tunnel.
---------------------------	------------	---

---

## tag-switching cos-map

To create a class map that specifies how classes map to label VCs when combined with a prefix map, use the **tag-switching cos-map** command in global configuration mode.

**tag-switching cos-map** *number*

---

<b>Syntax Description</b>	<i>number</i>	Unique number for a QoS map (from 1 to 255).
---------------------------	---------------	--

---

## tag-switching ip (global configuration)

To allow label switching of IPv4 packets, use the **tag-switching ip** command in global configuration mode. To disable IP Label Switching across all interfaces, use the **no** form of this command.

**tag-switching ip**

**no tag-switching ip**

---

**Syntax Description** This command has no arguments or keywords.

## tag-switching ip (interface configuration)

To enable label switching of IPv4 packets on an interface, use the **tag-switching ip** command in interface configuration mode. To disable IP label switching on this interface, use the **no** form of this command.

**tag-switching ip**

**no tag-switching ip**

---

**Syntax Description** This command has no arguments or keywords.

## tag-switching ip default-route

To enable the distribution of labels associated with the IP default route, use the **tag-switching ip default-route** command in global configuration mode.

**tag-switching ip default-route**

---

**Syntax Description** This command has no arguments or keywords.

## tag-switching mtu

To override the per-interface maximum transmission unit (MTU), use the **tag-switching mtu** command in interface configuration mode. To restore the default, use the **no** form of this command.

**tag-switching mtu** *bytes*

**no tag-switching mtu**

---

**Syntax Description** *bytes* MTU (in bytes).

---

## tag-switching prefix-map

To configure a router to use a specified QoS map when a label destination prefix matches the specified access list, use the **tag-switching prefix-map** command in ATM subinterface configuration submode.

```
tag-switching prefix-map prefix-map access-list access-list cos-map cos-map
```

### Syntax Description

<i>prefix-map</i>	A unique number for a prefix map.
<b>access-list</b> <i>access list</i>	A unique number for a simple IP access list.
<b>cos-map</b> <i>cos-map</i>	A unique number for a CoS map.

## tag-switching request-tags for

To restrict the creation of LVCs through the use of access lists on the LSC or label edge router, use the **tag-switching request-tags for** global configuration command. To disable this feature, use the **no** form of this command.

```
tag-switching request-tags for access-list
```

```
no tag-switching request-tags for
```

### Syntax Description

<i>access-list</i>	A named or numbered standard IP access list.
--------------------	--

## tag-switching tag-range downstream

To configure the size of the label (tag) space for downstream unicast label allocation, use the **tag-switching tag-range downstream** command in global configuration mode. To revert the platform defaults, use the **no** form of this command.

```
tag-switching tag-range downstream min max reserved
```

```
no tag-switching tag-range downstream min max reserved
```

### Syntax Description

<i>min</i>	The smallest label allowed in the label space. The default is 10.
<i>max</i>	The largest label allowed in the label space. The default is 10000.
<i>reserved</i>	The number of labels reserved for diagnostic purposes. These labels come out of the low end of the label space. The default is 16.

## tag-switching tdp discovery

To configure the interval between transmission of LDP (TDP) discovery hello messages, or the hold time for a LDP transport connection, use the **tag-switching tdp discovery** command in global configuration mode.

```
tag-switching tdp discovery {hello | directed hello} {holdtime | interval} seconds
```

Syntax Description		
<b>hello</b>		Configures the intervals and hold times for directly connected neighbors.
<b>directed-hello</b>		Configures the intervals and hold times for neighbors that are not directly connected (for example, LDP sessions that run through a LSP tunnel).
<b>holdtime</b>		The interval for which a connection stays up if no hello messages are received. The default is 15 seconds.
<b>interval</b>		The period between the sending of consecutive hello messages. The default is 5 seconds.
<i>seconds</i>		The hold time or interval.

## tag-switching tdp holdtime

To enable LSP tunnel functionality on a device, use the **tag-switching tdp holdtime** command in global configuration mode.

```
tag-switching tdp holdtime seconds
```

Syntax Description		
<i>seconds</i>		The time for which an LDP session is maintained in the absence of LDP messages from the session peer device.

## tag-switching tsp-tunnels (global configuration)

To allow the operation of Label-Switched Path (LSP) tunnels, use the **tag-switching tsp-tunnels** command in global configuration mode. To disable the operation of LSP tunnels, use the **no** form of this command.

```
tag-switching tsp-tunnels
```

```
no tag-switching tsp-tunnels
```

Syntax Description	
	This command has no arguments or keywords.

## tag-switching tsp-tunnels (interface configuration)

To allow Label-Switched Path (LSP) tunnel operation over an interface, use the **tag-switching tsp-tunnels** command in interface configuration mode. To disable LSP tunnel operation over an interface, use the **no** form of this command.

**tag-switching tsp-tunnels**

**no tag-switching tsp-tunnels**

**Syntax Description** This command has no arguments or keywords.

## traffic-engineering filter

To specify a filter with the given number and properties, use the **traffic-engineering filter** command in router configuration mode. To disable this function, use the **no** form of this command.

**traffic-engineering filter** *filter-number* **egress** *ip-address mask*

**no traffic-engineering filter**

<b>Syntax Description</b>	<i>filter-number</i>	A decimal value representing the number of the filter.
	<b>egress</b> <i>ip-address mask</i>	IP address and mask for the egress port.

## traffic-engineering route

To configure a route for a specified filter through a specified tunnel, use the **traffic-engineering route** command in router configuration mode. To disable this function, use the **no** form of this command.

**traffic-engineering route** *filter-number interface* [**preference** *number*] [**loop-prevention** {**on** | **off**}]

**no traffic-engineering route** *filter-number interface* [**preference** *number*] [**loop-prevention** {**on** | **off**}]

<b>Syntax Description</b>	<i>filter-number</i>	The number of the traffic engineering filter to be forwarded through the use of this traffic engineering route, if the route is installed.
	<i>interface</i>	LSP-encapsulated tunnel on which the traffic-passing filter should be sent, if this traffic engineering route is installed.
	<b>preference</b> <i>number</i>	(Optional) This is a number from 1 to 255, with a lower value being more desirable. The default is 1.
	<b>loop-prevention</b>	(Optional) A setting of <b>on</b> or <b>off</b> . The default is <b>on</b> .

## tunnel mode mpls traffic-eng

To set the mode of a tunnel to MPLS for traffic engineering, use the **tunnel mode mpls traffic-eng** interface configuration command. To disable this feature, use the **no** form of this command.

**tunnel mode mpls traffic-eng**

**no tunnel mode mpls traffic-eng**

---

**Syntax Description** This command has no arguments or keywords.

## tunnel mode tag-switching

To set the encapsulation mode of the tunnel to label switching, use the **tunnel mode tag-switching** command in interface configuration mode. To set the tunneling encapsulation mode to the default, use the **no** form of this command.

**tunnel mode tag-switching**

**no tunnel mode tag-switching**

---

**Syntax Description** This command has no arguments or keywords.

## tunnel mpls traffic-eng affinity

To configure an affinity (the properties the tunnel requires in its links) for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng affinity** interface configuration command. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng affinity** *properties* [**mask** *mask value*]

**no tunnel mpls traffic-eng affinity** *properties* [**mask** *mask value*]

---

<b>Syntax Description</b>	<i>properties</i>	Attribute values required for links carrying this tunnel. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
	<b>mask</b> <i>mask value</i>	(Optional) Link attribute to be checked. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

---

## tunnel mpls traffic-eng autoroute announce

To specify that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **tunnel mpls traffic-eng autoroute announce** interface configuration command. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng autoroute announce**

**no tunnel mpls traffic-eng autoroute announce**

**Syntax Description** This command has no arguments or keywords.

## tunnel mpls traffic-eng autoroute metric

To specify the MPLS traffic engineering tunnel metric that the IGP enhanced SPF calculation uses, use the **tunnel mpls traffic-eng autoroute metric** interface configuration command. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng autoroute metric** {**absolute** | **relative**} *value*

**no tunnel mpls traffic-eng autoroute metric**

<b>Syntax Description</b>	<b>absolute</b>	Absolute metric mode; you can enter a positive metric value.
	<b>relative</b>	Relative metric mode; you can enter a positive, negative, or zero value.
	<i>value</i>	The metric that the IGP enhanced SPF calculation uses. The <b>relative</b> value can be from -10 to 10.

## tunnel mpls traffic-eng bandwidth

To configure the bandwidth required for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng bandwidth** interface configuration command. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng bandwidth** *bandwidth*

**no tunnel mpls traffic-eng bandwidth** *bandwidth*

<b>Syntax Description</b>	<i>bandwidth</i>	The bandwidth required for an MPLS traffic engineering tunnel. Bandwidth is specified in kbps.
---------------------------	------------------	--

## tunnel mpls traffic-eng path-option

To configure a path option for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng path-option** interface configuration command. To disable this feature, use the **no** form of this command.

```
tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name |  
path-number}} [lockdown]
```

```
no tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name |  
path-number}} [lockdown]
```

### Syntax Description

<i>number</i>	When multiple path options are configured, lower numbered options are preferred.
<b>dynamic</b>	Path of the LSP is dynamically calculated.
<b>explicit</b>	Path of the LSP is an IP explicit path.
<b>name</b> <i>path-name</i>	Path name of the IP explicit path that the tunnel uses with this option.
<i>path-number</i>	Path number of the IP explicit path that the tunnel uses with this option.
<b>lockdown</b>	(Optional) The LSP cannot be reoptimized.

## tunnel mpls traffic-eng priority

To configure the setup and reservation priority for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng priority** interface configuration command. To disable this feature, use the **no** form of this command.

```
tunnel mpls traffic-eng priority setup-priority [hold-priority]
```

```
no tunnel mpls traffic-eng priority setup-priority [hold-priority]
```

### Syntax Description

<i>setup-priority</i>	The priority used when signalling an LSP for this tunnel to determine which existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
<i>hold-priority</i>	(Optional) The priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signalled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

## tunnel tsp-hop

To define hops in the path for the label switching tunnel, use the **tunnel tsp-hop** command in interface configuration mode. To remove these hops, use the **no** form of this command.

**tunnel tsp-hop** *hop-number ip-address* [**lasthop**]

**no tunnel tsp-hop** *hop-number ip-address* [**lasthop**]

---

### Syntax Description

---

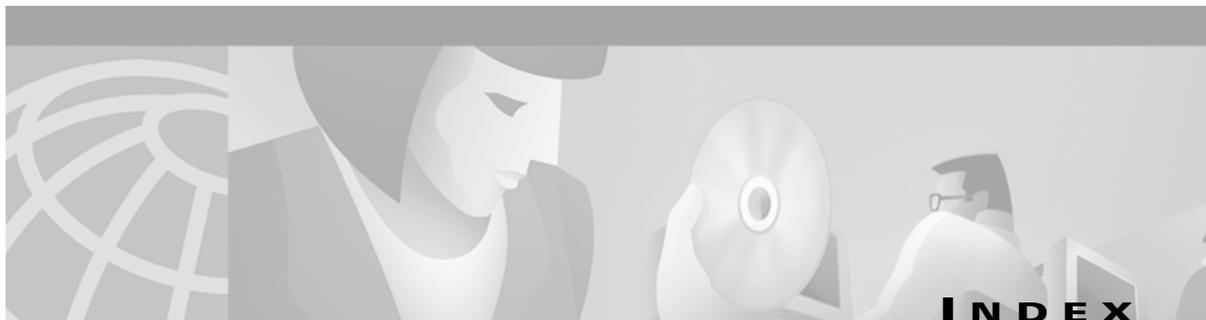
<i>hop-number</i>	The sequence number of the hop being defined in the path. The first number is 1, which identifies the hop just after the head hop.
<i>ip-address</i>	The IP address of the input interface on that hop.
<b>lasthop</b>	(Optional) Indicates that the hop being defined is the final hop in the path (the tunnel destination).

---



## **Index**





---

<b>BC</b>	Cisco IOS Bridging and IBM Networking Configuration Guide
<b>CS1</b>	Cisco IOS Command Summary, Volume 1 of 3
<b>CS2</b>	Cisco IOS Command Summary, Volume 2 of 3
<b>CS3</b>	Cisco IOS Command Summary, Volume 3 of 3
<b>DC</b>	Cisco IOS Dial Technologies Configuration Guide
<b>FC</b>	Cisco IOS Configuration Fundamentals Configuration Guide
<b>IC</b>	Cisco IOS Interface Configuration Guide
<b>IPC</b>	Cisco IOS IP Routing Configuration Guide
<b>MWC</b>	Cisco IOS Mobile Wireless Configuration Guide
<b>P2C</b>	Cisco IOS AppleTalk and Novell IPX Configuration Guide
<b>P3C</b>	Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide
<b>QC</b>	Cisco IOS Quality of Service Solutions Configuration Guide
<b>SC</b>	Cisco IOS Security Configuration Guide
<b>TC</b>	Cisco IOS Terminal Services Configuration Guide
<b>VC</b>	Cisco IOS Voice, Video, and Fax Configuration Guide
<b>WC</b>	Cisco IOS Wide-Area Networking Configuration Guide
<b>XC</b>	Cisco IOS Switching Services Configuration Guide

---

## A

aaa accounting command CS2-159  
aaa accounting connection h323 command CS2-161  
aaa accounting nested command CS2-162  
aaa accounting resource start-stop failure command CS2-162  
aaa accounting resource start-stop group command CS2-162  
aaa accounting resource stop-failure group command CS2-163  
aaa accounting send stop-record authentication failure command CS2-163  
aaa accounting suppress null-username command CS2-164  
aaa accounting update command CS2-164  
aaa authentication arap command CS2-139  
aaa authentication banner command CS2-140

aaa authentication enable default command CS2-140  
aaa authentication fail-message command CS2-141  
aaa authentication login command CS2-141  
aaa authentication nasi command CS2-142  
aaa authentication password-prompt command CS2-143  
aaa authentication ppp command CS2-143  
aaa authentication username-prompt command CS2-144  
aaa authorization command CS2-155  
aaa authorization config-commands command CS2-156  
aaa authorization configuration default command CS2-391  
aaa authorization reverse-access command CS2-156  
aaa dnis map accounting network command CS2-164  
aaa dnis map authentication ppp group command CS2-144  
aaa dnis map authorization network group command CS2-157  
aaa group server command CS2-183  
aaa group server radius command CS2-169  
aaa group-configuration command CS2-391  
aaa nas port extended command CS2-169  
aaa new-model command CS2-145  
aaa pod server command CS2-145  
aaa preauth command CS2-146  
aaa processes command CS2-146  
aaa route download command CS2-392  
aaa session-mib command CS2-165  
abr command CS2-3  
absolute-timeout command CS2-591  
accept dialin command CS2-392  
accept dialout command CS2-392  
access-class (LAT) command CS2-591  
access-class command CS2-101  
access-enable command CS2-193  
access-list dynamic-extend command CS2-193  
access-list rate-limit command CS2-655  
access-profile command CS2-146

access-template command CS2-194  
accounting (gatekeeper) command CS2-166  
address command CS2-243  
addressed-key command CS2-243  
address-family command CS2-656  
append-after command CS2-656  
aps authenticate command CS2-275  
aps force command CS2-275  
aps group command CS2-276  
aps lockout command CS2-276  
aps manual command CS2-276  
aps protect command CS2-276  
aps revert command CS2-277  
aps timers command CS2-277  
aps unidirectional command CS2-277  
aps working command CS2-278  
arap authentication command CS2-147  
arap callback command CS2-393  
arap dedicated command CS2-592  
arap enable command CS2-592  
arap net-access-list command CS2-592  
arap network command CS2-593  
arap noguest command CS2-593  
arap require-manual-password command CS2-593  
arap timelimit command CS2-594  
arap warningtime command CS2-594  
arap zonelist command CS2-594  
arp command CS2-95  
async default ip address command  
    *See* peer default ip address command  
async default routing command CS2-393  
async dynamic address command CS2-393  
async dynamic routing command CS2-394  
async mode dedicated command CS2-394  
async mode interactive command CS2-394  
atm aal aal3/4 command CS2-3  
atm abr rate-factors command CS2-4  
atm address-registration command CS2-4  
atm arp-server command CS2-4  
atm clock internal command CS2-5  
atm ds3-scrumble command CS2-5  
atm e164 auto-conversion command CS2-5  
atm e3-scrumble command CS2-6  
atm esi-address command CS2-6  
atm exception-queue command CS2-6  
atm framing (DS3) command CS2-7  
atm framing (E3) command CS2-7  
atm ilmi-keepalive command CS2-7  
atm ilmi-pvc-discovery command CS2-8  
atm lbo command CS2-8  
atm max channels command CS2-8  
atm max-channels command CS2-8  
atm maxvc command CS2-9  
atm mid-per-vc command CS2-9  
atm multicast command CS2-9  
atm multipoint-interval command CS2-9  
atm multipoint-signalling command CS2-10  
atm nsap-address command CS2-10  
atm oam flush command CS2-10  
atm oversubscribe command CS2-11  
atm pvp command CS2-11  
atm rate-queue command CS2-11  
atm rawq-size command CS2-12  
atm route-bridge command CS2-51  
atm rxbuff command CS2-13  
atm sig-traffic-shaping strict command CS2-14  
atm smds-address command CS2-14  
atm sonet command CS2-278  
atm sonet stm-1 command CS2-14  
atm txbuff command CS2-15  
atm uni-version command CS2-15  
atm vc-per-vp command CS2-15  
atm vp-filter command CS2-16  
atm-address command CS2-657  
atmsig close atm command CS2-13  
authen before-forward command CS2-395  
authentication (IKE policy) command CS2-244  
authorization command CS2-157

autocommand command CS2-395, CS2-595  
 autodetect encapsulation command CS2-395  
 autohangup command CS2-396  
 auto-polarity command CS2-278  
 autoselect command CS2-396

---

## B

backup command CS2-396  
 backup delay command CS2-397  
 backup interface command CS2-397  
 backup interface dialer command CS2-398  
 backup load command CS2-398  
 bandwidth interface command CS2-279  
 bert abort command CS2-279  
 bert controller command CS2-279  
 bert pattern command CS2-280  
 bert profile command CS2-280  
 bfe command CS2-101  
 bgp default route-target filter command CS2-657  
 BGP neighbor connections CS2-712  
 bgp scan-time command CS2-657  
 broadcast command CS2-16  
 busy-message command CS2-595  
 busyout (port) command CS2-399  
 busyout (spe) command CS2-399  
 busyout command CS2-398

---

## C

cable bundle command CS2-658  
 cable helper-address command CS2-658  
 cablelength command CS2-281  
 cablelength long command CS2-282  
 cablelength short command CS2-282  
 cache command CS2-658  
 call guard-timer command CS2-170  
 call progress tone country command CS2-399

callback forced-wait command CS2-400  
 called-number command CS2-400  
 calltracker call-record command CS2-400  
 calltracker enable command CS2-401  
 calltracker history max-size command CS2-401  
 calltracker history retain-mins command CS2-401  
 call-type cas command CS2-402  
 call-type command CS2-402  
 carrier-delay command CS2-283  
 cas-custom command CS2-402  
 cas-group (e1 controller) command CS2-403  
 cas-group (t1 controller) command CS2-404  
 cbr command CS2-16  
 certificate command CS2-235  
 ces aal1 clock command CS2-17  
 ces aal1 service command CS2-17  
 ces circuit command CS2-18  
 ces command CS2-17  
 ces dsx1 clock source command CS2-19  
 ces dsx1 framing command CS2-19  
 ces dsx1 lbo command CS2-20  
 ces dsx1 linecode command CS2-20  
 ces dsx1 loopback command CS2-20  
 ces dsx1 signalmode robbedbit command CS2-21  
 ces partial-fill command CS2-21  
 ces pvc command CS2-21  
 ces-cdv command CS2-18  
 channel-group (Fast EtherChannel) command CS2-283  
 channel-group command CS2-406  
 chat-script command CS2-407  
 class (map-list configuration) command CS2-57  
 class (MPLS) command CS2-659  
 class (virtual circuit configuration) command CS2-58  
 class command CS2-407  
 class-int command CS2-22  
 class-range command CS2-51  
 class-vc command CS2-22  
 clear access-template command CS2-194  
 clear adjacency command CS2-659

- clear aim command CS2-283
- clear atm vc command CS2-659
- clear cef linecard command CS2-660
- clear controller command CS2-407
- clear controller lex command CS2-283
- clear cot summary command CS2-408
- clear counters (async) command CS2-408
- clear counters command CS2-284
- clear counters line command CS2-408
- clear crypto isakmp command CS2-244
- clear crypto sa command CS2-225
- clear dialer command CS2-408
- clear dialer dnis command CS2-409
- clear dialer sessions command CS2-409
- clear dsip tracing command CS2-409
- clear entry command CS2-595
- clear frame-relay-inarp command CS2-58
- clear hub command CS2-285
- clear hub counters command CS2-286
- clear interface command CS2-286, CS2-410
- clear interface fastethernet command CS2-288
- clear interface serial command CS2-288
- clear interface virtual-access command CS2-410
- clear ip audit configuration command CS2-211
- clear ip audit statistics command CS2-211
- clear ip auth-proxy cache command CS2-219
- clear ip cef command CS2-660
- clear ip cef prefix-statistics command CS2-660
- clear ip flow stats command CS2-660
- clear ip mds forwarding command CS2-661
- clear ip mroute command CS2-661
- clear ip pim interface count command CS2-661
- clear ip route download command CS2-410
- clear ip route vrf command CS2-661
- clear ip trigger-authentication command CS2-148
- clear kerberos creds command CS2-187
- clear lane le-arp command CS2-662
- clear lane server command CS2-663
- clear line async-queue command CS2-411
- clear line command CS2-410
- clear modem command CS2-411
- clear modem counters command CS2-411
- clear modempool-counters command CS2-412
- clear mpoa client cache command CS2-663
- clear mpoa server cache command CS2-664
- clear port command CS2-412
- clear port log command CS2-412
- clear resource-pool command CS2-413
- clear rlm group command CS2-413
- clear service-module serial command CS2-288
- clear snapshot quiet-time command CS2-413
- clear spe command CS2-414
- clear spe counters command CS2-414
- clear spe log command CS2-415
- clear vpdn history failure command CS2-415
- clear vpdn tunnel command CS2-415
- clear x25 command CS2-101
- clear x25-vc command CS2-102
- clear xot command CS2-102
- clid command CS2-170
- clid group command CS2-416
- client-atm-address command CS2-664
- client-atm-address name command CS2-664
- clock rate command CS2-289
- clock source (Cisco AS5200) command CS2-289
- clock source (Cisco MC3810) command CS2-291
- clock source (controller) command CS2-290
- clock source (CT3IP) command CS2-290
- clock source (interface) command CS2-291
- clock source command CS2-416
- clock source line command CS2-416
- clp-bit command CS2-91
- cmns enable command CS2-102
- cmt connect command CS2-292
- cmt disconnect command CS2-292
- community-list command CS2-712
- compress command CS2-292
- compress mppc command CS2-294

compress predictor command  
     *See* compress command  
 compress stac caim command CS2-294  
 connect (Frame Relay) command CS2-58  
 connect (FR-ATM) command CS2-91, CS2-92  
 connect command CS2-596  
 controller command CS2-416  
 controller t1 command CS2-294  
 controller t3 command CS2-295  
 copy flash lex command CS2-295  
 copy modem command CS2-417  
 copy tftp lex command CS2-296  
 corlist incoming command CS2-417  
 corlist outgoing command CS2-417  
 cpp authentication command CS2-418  
 cpp callback accept command CS2-418  
 crc bits 5 command CS2-297  
 crc command CS2-296  
 crc4 command CS2-296  
 crl optional command CS2-235  
 crl query command CS2-236  
 crypto ca authenticate command CS2-236  
 crypto ca certificate chain command CS2-236  
 crypto ca certificate query command CS2-237  
 crypto ca crl request command CS2-237  
 crypto ca enroll command CS2-237  
 crypto ca identity command CS2-238  
 crypto ca trusted-root command CS2-238  
 crypto dynamic-map command CS2-226  
 crypto ipsec security-association lifetime command  
     CS2-226  
 crypto ipsec transform-set command CS2-226  
 crypto isakmp enable command CS2-245  
 crypto isakmp identity command CS2-245  
 crypto isakmp key command CS2-245  
 crypto isakmp policy command CS2-246  
 crypto key generate rsa (CA) command CS2-238  
 crypto key generate rsa (IKE) command CS2-246  
 crypto key pubkey-chain rsa command CS2-246

crypto key zeroize rsa command CS2-238  
 crypto map (IPSec global) command CS2-227  
 crypto map (IPSec interface) command CS2-227  
 crypto map client authentication list command CS2-247  
 crypto map client configuration address command  
     CS2-247  
 crypto map isakmp authorization list command CS2-247  
 crypto map local-address command CS2-227  
 ctype command CS2-171  
 cut-through command CS2-297

---

## D

deadtime (server-group configuration) command CS2-171  
 de-bit command CS2-92  
 de-bit map-clp command CS2-93  
 default (VPDN) command CS2-418  
 default command CS2-665  
 default-name command CS2-665  
 delay (interface) command CS2-298  
 description (controller) command CS2-298  
 description (vpdn-group) command CS2-419  
 description command CS2-419  
 dialer aaa command CS2-172  
 dialer callback-secure command CS2-420  
 dialer callback-server command CS2-420  
 dialer called command CS2-421  
 dialer caller command CS2-421  
 dialer clid group command CS2-421  
 dialer command CS2-420  
 dialer congestion threshold command CS2-422  
 dialer dnis group command CS2-422  
 dialer dns command CS2-422  
 dialer dtr command CS2-423  
 dialer enable-timeout command CS2-423  
 dialer fast-idle (interface configuration) command  
     CS2-423  
 dialer fast-idle (map-class dialer configuration) command  
     CS2-424

- dialer hold-queue command CS2-424
  - dialer idle-timeout (interface configuration) command CS2-425
  - dialer in-band command CS2-425
  - dialer isdn command CS2-425
  - dialer isdn short-hold command CS2-426
  - dialer load-threshold command CS2-427
  - dialer map (AOC) command CS2-429
  - dialer map (SPC) command CS2-430
  - dialer map bridge command CS2-428
  - dialer map command CS2-428
  - dialer map snapshot command CS2-430
  - dialer max-link command CS2-431
  - dialer outgoing command CS2-431
  - dialer pool command CS2-431
  - dialer pool-member command CS2-432
  - dialer priority command CS2-432
  - dialer redial command CS2-432
  - dialer remote-name command CS2-433
  - dialer reserved-links command CS2-433
  - dialer rotary-group command CS2-433
  - dialer rotor command CS2-434
  - dialer string (dialer profiles) command CS2-434
  - dialer string (legacy DDR) command CS2-435
  - dialer string command CS2-434
  - dialer voice-call command CS2-435
  - dialer vpdn command CS2-435
  - dialer wait-for-carrier-time (interface configuration) command CS2-436
  - dialer wait-for-carrier-time (map-class dialer configuration) command CS2-436
  - dialer watch-disable command CS2-436
  - dialer watch-group command CS2-437
  - dialer watch-list command CS2-437
  - dialer-group command CS2-424
  - dialer-list protocol command CS2-426
  - dial-peer cor custom command CS2-437
  - dial-peer cor list command CS2-438
  - dial-shelf split backplane-ds0 command CS2-438
  - dial-shelf split slots command CS2-439
  - dial-shelf split slots none command CS2-439
  - dial-shelf split slots remove command CS2-439
  - dial-tdm-clock command CS2-440
  - disconnect command CS2-440
  - disconnect ssh command CS2-269
  - dnis (AAA preauthentication configuration) command CS2-172
  - dnis bypass (AAA preauthentication configuration) command CS2-173
  - dnis (preauthentication) command CS2-148
  - dnis (VPDN group configuration) command CS2-440
  - dnis group command CS2-441
  - dnsix-dmtp retries command CS2-259
  - dnsix-nat authorized-redirect command CS2-259
  - dnsix-nat primary command CS2-260
  - dnsix-nat secondary command CS2-260
  - dnsix-nat source command CS2-260
  - dnsix-nat transmit-count command CS2-261
  - domain command CS2-441
  - down-when-looped command CS2-298
  - ds0 busyout command CS2-442
  - ds0 busyout-threshold command CS2-442
  - ds0-group (controller e1) command CS2-442
  - dsu bandwidth command CS2-299
  - dsu mode command CS2-299
  - dte-invert-txc command CS2-299
  - duplex command CS2-300
  - dxl map command CS2-22
  - dxl pvc command CS2-23
- 
- E**
- e2-clockrate command CS2-300
  - early-token-release command CS2-300
  - efci-bit command CS2-93
  - enable password command CS2-251
  - enable secret command CS2-252
  - enabled command CS2-665
  - encapsulation aal5 command CS2-23

encapsulation atm-dxi command CS2-24  
 encapsulation command CS2-301  
 encapsulation cpp command CS2-445  
 encapsulation dot1q command CS2-665  
 encapsulation frame-relay command CS2-58  
 encapsulation isl command CS2-666  
 encapsulation lapb command CS2-103  
 encapsulation sde command CS2-666  
 encapsulation smds command CS2-95  
 encapsulation tr-isl trbrf-vlan command CS2-666  
 encapsulation x25 command CS2-103  
 encryption (IKE policy) command CS2-248  
 encryption mppe command CS2-445  
 enrollment mode ra command CS2-239  
 enrollment retry-count command CS2-239  
 enrollment retry-period command CS2-239  
 enrollment url command CS2-240  
 evaluate command CS2-195  
 exit command CS2-666  
 exit-address-family command CS2-667  
 export destination command CS2-667  
 extended-port command CS2-667

---

## F

fddi burst-count command CS2-301  
 fddi c-min command CS2-302  
 fddi cmt-signal-bits command CS2-302  
 fddi duplicate-address-check command CS2-303  
 fddi encapsulate command CS2-303  
 fddi frames-per-token command CS2-304  
 fddi smt-frames command CS2-304  
 fddi tb-min command CS2-304  
 fddi tl-min-time command CS2-305  
 fddi token-rotation-time command CS2-305  
 fddi t-out command CS2-305  
 fddi valid-transmission-time command CS2-306  
 fdl command CS2-306  
 firmware location command CS2-446  
 firmware upgrade command CS2-446  
 flowcontrol command CS2-446  
 force-local-chap command CS2-447  
 frame-relay adaptive-shaping command CS2-60  
 frame-relay address registration auto-address command CS2-60  
 frame-relay address registration ip command CS2-60  
 frame-relay address-reg enable command CS2-61  
 frame-relay bc command CS2-61  
 frame-relay be command CS2-61  
 frame-relay broadcast-queue command CS2-62  
 frame-relay cir command CS2-62  
 frame-relay class command CS2-62  
 frame-relay command CS2-307  
 frame-relay congestion threshold de command CS2-63  
 frame-relay congestion threshold ecn command CS2-63  
 frame-relay congestion-management command CS2-63  
 frame-relay custom-queue-list command CS2-64  
 frame-relay de-group command CS2-64  
 frame-relay de-list command CS2-64  
 frame-relay end-to-end keepalive error-threshold command CS2-65  
 frame-relay end-to-end keepalive event-window command CS2-66  
 frame-relay end-to-end keepalive mode command CS2-66  
 frame-relay end-to-end keepalive success-events command CS2-66  
 frame-relay end-to-end keepalive timer command CS2-67  
 frame-relay fragment command CS2-68  
 frame-relay frmr command CS2-71  
 frame-relay holdq command CS2-68  
 frame-relay idle-timer command CS2-68  
 frame-relay interface-dlci command CS2-69  
 frame-relay interface-dlci switched command CS2-70  
 frame-relay intf-type command CS2-70  
 frame-relay inverse-arp command CS2-70  
 frame-relay ip tcp header-compression command CS2-71  
 frame-relay lapf k command CS2-72  
 frame-relay lapf n200 command CS2-72  
 frame-relay lapf n201 command CS2-72

frame-relay lapf t200 command CS2-73  
 frame-relay lapf-t203 command CS2-73  
 frame-relay lmi-n391dte command CS2-73  
 frame-relay lmi-n392dce command CS2-74  
 frame-relay lmi-n392dte command CS2-74  
 frame-relay lmi-n393dce command CS2-74  
 frame-relay lmi-n393dte commands CS2-75  
 frame-relay lmi-t392dce command CS2-75  
 frame-relay lmi-type command CS2-75  
 frame-relay local-dlci command CS2-76  
 frame-relay map bridge command CS2-77  
 frame-relay map clns command CS2-78  
 frame-relay map command CS2-76, CS2-307  
 frame-relay map ip tcp header-compression command CS2-78  
 frame-relay mincir command CS2-78  
 frame-relay multicast-dlci command CS2-79  
 frame-relay payload-compress command CS2-79  
 frame-relay payload-compress packet-by-packet command CS2-79  
 frame-relay policing command CS2-80  
 frame-relay priority-dlci-group command CS2-80  
 frame-relay priority-group command CS2-81  
 frame-relay pvc command CS2-81  
 frame-relay qos-autosense command CS2-82  
 frame-relay route command CS2-82  
 frame-relay svc command CS2-83  
 frame-relay switching command CS2-83  
 frame-relay tc command CS2-83  
 frame-relay traffic-rate command CS2-84  
 frame-relay traffic-shaping command CS2-84  
 framing (E1/T1 controller) command CS2-308  
 framing (E3/T3 interface) command CS2-309  
 framing (T3 controller) command CS2-309  
 framing command CS2-308, CS2-447  
 fr-atm connect dlci command CS2-59  
 full-duplex command CS2-310

---

**G**

group (AAA preauthentication configuration) command CS2-173  
 group (IKE policy) command CS2-248  
 group command CS2-148  
 group range command CS2-448

---

**H**

half-duplex command CS2-310  
 half-duplex controlled-carrier command CS2-310  
 half-duplex timer command CS2-311  
 hash (IKE policy) command CS2-248  
 holding-time command CS2-668  
 hold-queue command CS2-312  
 hssi external-loop-request command CS2-312  
 hssi internal-clock command CS2-312  
 hub command CS2-313  
 hw-module reload command CS2-448

---

**I**

idle-timeout command CS2-25  
 ignore-dcd command CS2-313  
 ignore-hw local-loopback command CS2-313  
 ima active-links-minimum command CS2-25  
 ima clock-mode command CS2-26  
 ima differential-delay-maximum command CS2-26  
 ima frame-length command CS2-26  
 ima test command CS2-27  
 ima-group command CS2-27  
 imli manage command CS2-25  
 import map command CS2-668  
 inarp command CS2-27  
 index command CS2-668  
 initiate-to command CS2-448  
 interface (RLM server) command CS2-449  
 interface atm command CS2-28, CS2-668

- interface atm ima command CS2-29
- interface bri command CS2-449
- interface cbr command CS2-29
- interface command CS2-314
- interface ctunnel command CS2-316
- interface dialer command CS2-450
- interface fastethernet command CS2-317 , CS2-669
- interface gigabitethernet command CS2-318
- interface group-async command CS2-318
- interface multilink command CS2-450
- interface port-channel command CS2-318
- interface pos command CS2-319
- interface serial command CS2-451
- interface serial multipoint command CS2-96
- interface vg-anylan command CS2-319
- interface virtual-template command CS2-451
- interface XTagATM command CS2-670
- international bit command CS2-320
- invert data command CS2-320
- invert rxclock command CS2-320
- invert txclock command CS2-321
- invert-transmit-clock command
  - See* invert txclock command
- ip address negotiated command CS2-451
- ip address-pool command CS2-451
- ip alias command CS2-598
- ip audit attack command CS2-212
- ip audit command CS2-212
- ip audit info command CS2-212
- ip audit name command CS2-213
- ip audit notify command CS2-213
- ip audit po local command CS2-214
- ip audit po max-events command CS2-214
- ip audit po protected command CS2-214
- ip audit po remote command CS2-215
- ip audit signature command CS2-216
- ip audit smtp command CS2-216
- ip auth-proxy auth-cache-time command CS2-220
- ip auth-proxy auth-proxy-banner command CS2-220
- ip auth-proxy command CS2-219
- ip auth-proxy name command CS2-220
- ip cache-invalidate-delay command CS2-670
- ip cef accounting command CS2-671
- ip cef command CS2-670
- ip cef distributed command CS2-670
- ip cef traffic-statistics command CS2-671
- ip dhcp relay information option command CS2-671
- ip dhcp-server command CS2-452
- ip director default-weights command CS2-321
- ip director dfp command CS2-322
- ip director dfp security command CS2-323
- ip director host priority command CS2-323
- ip director host weights command CS2-325
- ip director server availability command CS2-326
- ip director server port availability command CS2-327
- ip explicit-path command CS2-672
- ip flow-aggregation cache command CS2-672
- ip flow-cache entries command CS2-672
- ip flow-export command CS2-673
- ip inspect (interface configuration) command CS2-204
- ip inspect alert-off command CS2-203
- ip inspect audit trail command CS2-203
- ip inspect dns-timeout command CS2-204
- ip inspect max-incomplete high command CS2-204
- ip inspect max-incomplete low command CS2-205
- ip inspect name command CS2-205
- ip inspect one-minute high command CS2-207
- ip inspect one-minute low command CS2-207
- ip inspect tcp finwait-time command CS2-208
- ip inspect tcp idle-time command CS2-208
- ip inspect tcp max-incomplete host command CS2-208
- ip inspect tcp synwait-time command CS2-209
- ip inspect udp idle-time command CS2-209
- ip load-sharing command CS2-673
- ip local-pool command CS2-598
- ip mroute-cache command CS2-674
- ip port-map command CS2-223
- ip radius source-interface command CS2-173

- ip reflexive-list timeout command CS2-195
- ip route command CS2-452
- ip route vrf command CS2-675
- ip route-cache cef command CS2-675
- ip route-cache command CS2-674
- ip route-cache flow command CS2-675
- ip rtp reserve command CS2-453
- ip security add command CS2-261
- ip security aeso command CS2-261
- ip security allow-reserved command CS2-266
- ip security dedicated command CS2-262
- ip security eso-info command CS2-263
- ip security eso-max command CS2-263
- ip security eso-min command CS2-263
- ip security extended-allowed command CS2-264
- ip security first command CS2-264
- ip security ignore-authorities command CS2-264
- ip security implicit-labelling command CS2-265
- ip security multilevel command CS2-265
- ip security strip command CS2-266
- ip ssh command CS2-269
- ip tacacs source-interface command CS2-183
- ip tcp async-mobility server command CS2-453
- ip tcp intercept connection-timeout command CS2-199
- ip tcp intercept drop-mode command CS2-199
- ip tcp intercept finrst-timeout command CS2-200
- ip tcp intercept list command CS2-200
- ip tcp intercept max-incomplete high command CS2-200
- ip tcp intercept max-incomplete low command CS2-201
- ip tcp intercept mode command CS2-201
- ip tcp intercept one-minute high command CS2-201
- ip tcp intercept one-minute low command CS2-202
- ip tcp intercept watch-timeout command CS2-202
- ip telnet quiet command CS2-453
- ip trigger-authentication (global) command CS2-149
- ip trigger-authentication (interface) command CS2-149
- ip verify unicast reverse-path command CS2-267
- ip vrf command CS2-676
- ip vrf forwarding command CS2-676
- ipx compression cipx command CS2-454
- ipx nasi-server enable command CS2-598
- ipx ppp-client command CS2-454
- isdn all-incoming-calls-v120 command CS2-454
- isdn answer1 command CS2-455
- isdn answer2 command CS2-455
- isdn autodetect command CS2-455
- isdn bchan-number-order command CS2-456
- isdn busy command CS2-456
- isdn call interface command CS2-456
- isdn caller command CS2-457
- isdn calling-number command CS2-457
- isdn calling-pty command CS2-457
- isdn conference-code command CS2-458
- isdn disconnect interface command CS2-458
- isdn disconnect-cause command CS2-458
- isdn fast-rollover-delay command CS2-459
- isdn gateway-max-interworking command CS2-459
- isdn guard-timer command CS2-174
- isdn incoming-voice command. CS2-460
- isdn layer1-emulate command CS2-460
- isdn leased-line bri 128 command CS2-460
- isdn map command CS2-461
- isdn negotiate-bchan command CS2-461
- isdn not-end-to-end command CS2-461
- isdn nsf-service command CS2-462
- isdn outgoing-voice command CS2-462
- isdn overlap-receiving command CS2-462
- isdn piafs-enabled command CS2-463
- isdn point-to-point-setup command CS2-463
- isdn protocol-emulate command CS2-463
- isdn rlm-group command CS2-464
- isdn send-alerting command CS2-464
- isdn sending-complete command CS2-464
- isdn service command CS2-465
- isdn snmp busyout b-channel command CS2-465
- isdn spid1 command CS2-466
- isdn spid2 command CS2-466
- isdn switch-type (BRI) command CS2-466

isdn switch-type (PRI) command CS2-467  
 isdn t306 command CS2-468  
 isdn t310 command CS2-468  
 isdn tei-negotiation command CS2-468  
 isdn transfer-code command CS2-469  
 isdn twait-disable command CS2-469  
 isdn voice-priority command CS2-469  
 isdn x25 dchannel command CS2-470  
 isdn x25 static-tei command CS2-470

---

## K

keepalive (ATM) command CS2-85  
 keepalive command CS2-327  
 keepalive-lifetime command CS2-677  
 keepalive-time command CS2-677  
 kerberos clients mandatory command CS2-187  
 kerberos credentials forward command CS2-188  
 kerberos instance map command CS2-188  
 kerberos local-realm command CS2-188  
 kerberos preauth command CS2-189  
 kerberos realm command CS2-189  
 kerberos server command CS2-189  
 kerberos srvtab entry command CS2-190  
 kerberos srvtab remote command CS2-190  
 key config-key command CS2-191  
 keymap command CS2-599  
 keymap-type command CS2-599  
 key-string (IKE) command CS2-249

---

## L

l2f ignore-mid-sequence command CS2-470  
 l2tp drop out-of-order command CS2-471  
 l2tp flow-control backoff-queuesize command CS2-471  
 l2tp flow-control maximum-ato command CS2-471  
 l2tp flow-control receive-window command CS2-472  
 l2tp flow-control static-rtt command CS2-472  
 l2tp hidden command CS2-472  
 l2tp ip tos reflect command CS2-473  
 l2tp ip udp checksum command CS2-473  
 l2tp offset command CS2-473  
 l2tp tunnel authentication command CS2-474  
 l2tp tunnel hello command CS2-474  
 l2tp tunnel password command CS2-474  
 lane auto-config-atm-address command CS2-677  
 lane bus-atm-address command CS2-678  
 lane client command CS2-678  
 lane client flush command CS2-679  
 lane client mpoa client name command CS2-679  
 lane client mpoa server name command CS2-679  
 lane client-atm-address command CS2-678  
 lane config database command CS2-680  
 lane config-atm-address command CS2-680  
 lane database command CS2-680  
 lane fixed-config-atm-address command CS2-681  
 lane fssrp command CS2-681  
 lane global-lecs-address command CS2-683  
 lane le-arp command CS2-683  
 lane server-atm-address command CS2-684  
 lane server-bus command CS2-684  
 lapb interface-outage command CS2-103  
 lapb k command CS2-104  
 lapb modulo command CS2-104  
 lapb n1 command CS2-104  
 lapb n2 command CS2-104  
 lapb protocol command CS2-105  
 lapb t1 command CS2-105  
 lapb t4 command CS2-105  
 lat access-list command CS2-600  
 lat command CS2-599  
 lat enabled command CS2-600  
 lat group-list command CS2-601  
 lat host-buffers command CS2-601  
 lat ka-timer command CS2-601  
 lat node command CS2-602  
 lat out-group command CS2-602

- lat remote-modification command CS2-602
  - lat retransmit-limit command CS2-603
  - lat server-buffers command CS2-603
  - lat service enabled command CS2-604
  - lat service ident command CS2-604
  - lat service password command CS2-605
  - lat service rating command CS2-605
  - lat service rotary command CS2-605
  - lat service timer command CS2-606
  - lat service-announcements command CS2-603
  - lat service-group command CS2-604
  - lat service-responder command CS2-605
  - lat service-timer command CS2-606
  - lat vc-sessions command CS2-606
  - lat vc-timer command CS2-606
  - lbo command CS2-327
  - lcp renegotiation command CS2-475
  - lex burned-in-address command CS2-328
  - lex input-address-list command CS2-328
  - lex input-type-list command CS2-329
  - lex priority-group command CS2-329
  - lex retry-count command CS2-329
  - lex timeout command CS2-330
  - lifetime (IKE policy) command CS2-249
  - limit base-size command CS2-475
  - limit overflow-size command CS2-475
  - line command CS2-476
  - linecode command CS2-330
  - line-power command CS2-476
  - line-termination command CS2-330
  - link (RLM) command CS2-476
  - link-test command CS2-331
  - list command CS2-685
  - loadsharing command CS2-477
  - local name command CS2-477
  - local-lnm command CS2-331
  - login (line) command CS2-607
  - login authentication command CS2-150
  - login-string command CS2-607
  - loopback (ATM) command CS2-30
  - loopback (controller) command CS2-478
  - loopback (E3/T3 interface) command CS2-332
  - loopback (interface) command CS2-331
  - loopback (T1 interface) command CS2-332
  - loopback (T3 controller) command CS2-333
  - loopback applique command CS2-333
  - loopback command CS2-30
  - loopback dte command CS2-334
  - loopback interfaces CS2-315
  - loopback line command CS2-334
  - loopback local (controller) command CS2-478
  - loopback local (interface) command CS2-478
  - loopback remote (controller) command CS2-479
  - loopback remote (interface) command CS2-334
- 
- M**
- map-class atm command CS2-31
  - map-class dialer command CS2-479
  - map-class frame-relay command CS2-85
  - map-group command CS2-85
  - map-list command CS2-85
  - mask destination command CS2-685
  - mask source command CS2-685
  - match address (IPSec) command CS2-228
  - max bandwidth command CS2-52
  - max vc command CS2-52
  - maximum routes command CS2-685
  - media-type command CS2-336
  - media-type half-duplex command
    - See* half-duplex command
  - member (dial peer cor list) command CS2-480
  - member command CS2-479
  - metric-style narrow command CS2-686
  - metric-style transition command CS2-686
  - metric-style wide command CS2-687
  - mid command CS2-31
  - mls rp ip command CS2-687

- mls rp ip multicast command CS2-687
- mls rp ip multicast management-interface command CS2-688
- mls rp ipx (global) command CS2-688
- mls rp ipx (interface) command CS2-688
- mls rp locate ipx command CS2-688
- mls rp management-interface command CS2-689
- mls rp nde-address command CS2-689
- mls rp vlan-id command CS2-689
- mls rp vtp-domain command CS2-690
- mode (IPSec) command CS2-228
- modem answer-timeout command CS2-480
- modem at-mode command CS2-480
- modem at-mode-permit command CS2-481
- modem autoconfigure discovery command CS2-481
- modem autoconfigure type command CS2-481
- modem autotest command CS2-481
- modem bad command CS2-482
- modem buffer-size command CS2-482
- modem busyout command CS2-482
- modem busyout-threshold command CS2-483
- modem callin command CS2-483
- modem callout command CS2-483
- modem country mica command CS2-484
- modem country microcom\_hdms command CS2-485
- modem cts-required command
  - See* modem printer command
- modem dialin command CS2-487
- modem dtr-active command CS2-487
- modem hold-reset command CS2-488
- modem host command CS2-488
- modem inout command CS2-488
- modem link-info poll time command CS2-489
- modem min-speed max-speed command CS2-489
- modem poll retry command CS2-489
- modem poll time command CS2-490
- modem printer command CS2-490
- modem recovery action command CS2-490
- modem recovery maintenance command CS2-491
- modem recovery threshold command CS2-491
- modem recovery-time command CS2-492
- modem ri-is-cd command
  - See* modem dialin command
- modem shutdown command CS2-492
- modem startup-test command CS2-492
- modem status-poll command CS2-493
- modemcap edit command CS2-493
- modemcap entry command CS2-493
- modem-pool command CS2-494
- mop enabled command CS2-337
- mop sysid command CS2-337
- mpls atm control-vc command CS2-690
- mpls atm vpi command CS2-690
- mpls ip (global) command CS2-691
- mpls ip (interface configuration) command CS2-691
- mpls ip default-route command CS2-691
- mpls ip propagate-ttl command CS2-691
- mpls ip ttl-expiration pop command CS2-692
- mpls label range command CS2-692
- mpls mtu command CS2-692
- mpls traffic-eng administrative-weight command CS2-693
- mpls traffic-eng area command CS2-694
- mpls traffic-eng attribute-flags command CS2-694
- mpls traffic-eng command CS2-693
- mpls traffic-eng flooding thresholds command CS2-695
- mpls traffic-eng link timers bandwidth-hold command CS2-696
- mpls traffic-eng link timers periodic-flooding command CS2-696
- mpls traffic-eng link-management timers bandwidth-hold command CS2-695
- mpls traffic-eng link-management timers periodic-flooding command CS2-695
- mpls traffic-eng logging lsp command CS2-696
- mpls traffic-eng logging tunnel command CS2-697
- mpls traffic-eng reoptimize command CS2-697
- mpls traffic-eng reoptimize events command CS2-697
- mpls traffic-eng reoptimize timers frequency command CS2-698

mpls traffic-eng router-id command CS2-698  
 mpls traffic-eng signaling advertise implicit-null  
 command CS2-698  
 mpls traffic-eng tunnels (config) command CS2-699  
 mpls traffic-eng tunnels (configuration) command  
 CS2-699  
 mpls traffic-eng tunnels (interface) command CS2-699  
 mpoa client config name command CS2-699  
 mpoa client name command CS2-699  
 mpoa server config name command CS2-700  
 mpoa server name command CS2-700  
 mpoa server name trigger ip-address command CS2-700  
 mtu command CS2-337  
 multilink bundle-name command CS2-495  
 multilink virtual-template command CS2-496  
 multilink-group command  
*See ppp multilink group command*

---

## N

name (dial peer cor custom) command CS2-496  
 name elan-id command CS2-701  
 name local-seg-id command CS2-701  
 name preempt command CS2-701  
 name server-atm-address command CS2-702  
 named-key command CS2-249  
 nasi authentication command CS2-150  
 national bit command CS2-338  
 national reserve command CS2-338  
 negotiation command CS2-338  
 neighbor activate command CS2-702  
 neighbor allowas-in command CS2-702  
 neighbor as-override command CS2-703  
 netbios nbf command CS2-496  
 network-clock-priority command CS2-497  
 network-clock-select (ATM) command CS2-31  
 network-clock-select command CS2-497  
 network-id command CS2-703  
 next-address command CS2-703  
 no ip inspect command CS2-209  
 nrzi-encoding command CS2-339  
 number command CS2-497

---

## O

oam retry command CS2-32  
 oam-pvc command CS2-32  
 oam-range command CS2-52  
 oam-svc command CS2-33

---

## P

pad command CS2-608  
 password command CS2-252  
 password encryption CS2-255  
 peer default IP address command CS2-608  
 permission (dial peer voice) command CS2-498  
 permit (reflexive) command CS2-196  
 pool-member command CS2-498  
 pool-range command CS2-498  
 port command CS2-499  
 port (interface) command CS2-339  
 port modem autotest command CS2-499  
 pos ais-shut command CS2-340  
 pos flag command CS2-340  
 pos framing command CS2-340  
 pos framing-sdh command  
*See pos framing command*  
 pos internal-clock command  
*See clock source (CT3IP) command*  
 pos report command CS2-341  
 pos scramble-atm command CS2-342  
 pos threshold command CS2-342  
 posi framing-sdh command  
*See pos framing command*  
 ppp accounting command CS2-167  
 ppp authentication command CS2-150

- ppp authorization command CS2-158
  - ppp bap call command CS2-500
  - ppp bap callback command CS2-500
  - ppp bap drop command CS2-501
  - ppp bap link types command CS2-501
  - ppp bap max command CS2-501
  - ppp bap monitor load command CS2-502
  - ppp bap number command CS2-502
  - ppp bap timeout command CS2-503
  - ppp bridge appletalk command CS2-503
  - ppp bridge ip command CS2-503
  - ppp bridge ipx command CS2-504
  - ppp callback (DDR) command CS2-504
  - ppp callback (PPP client) command CS2-504
  - ppp chap hostname command CS2-151
  - ppp chap password command CS2-151
  - ppp chap refuse command CS2-152
  - ppp chap wait command CS2-152
  - ppp command CS2-500
  - ppp encrypt mppe command CS2-505
  - ppp ipcp command CS2-505
  - ppp lcp delay command CS2-506
  - ppp lcp fast-start command CS2-506
  - ppp link reorders command CS2-506
  - ppp max-bad-auth command CS2-507
  - ppp multilink command CS2-507
  - ppp multilink fragment delay command CS2-507
  - ppp multilink fragment disable command CS2-508
  - ppp multilink fragment maximum command CS2-508
  - ppp multilink group command CS2-508
  - ppp multilink idle-link command CS2-509
  - ppp multilink interleave command CS2-509
  - ppp multilink links maximum command CS2-509
  - ppp multilink links minimum command CS2-510
  - ppp multilink load-threshold command CS2-510
  - ppp pap command CS2-152
  - ppp pap sent-username command CS2-153
  - ppp quality command CS2-510
  - ppp reliable-link command CS2-511
  - ppp timeout authentication command CS2-511
  - ppp timeout command CS2-511
  - ppp timeout multilink link add command CS2-512
  - ppp timeout multilink link remove command CS2-512
  - ppp timeout multilink lost-fragment command CS2-512
  - ppp timeout ncp command CS2-513
  - ppp timeout retry command CS2-513
  - pppoe enable command CS2-53
  - pppoe limit per-mac command CS2-53
  - pppoe limit per-vc command CS2-53
  - pppoe limit per-vlan command CS2-54
  - pppoe max-session command CS2-54
  - pptp flow-control receive-window command CS2-513
  - pptp flow-control static-rtt command CS2-514
  - pptp tunnel echo command CS2-514
  - pri-group command CS2-343
  - pri-group timeslots nfas\_d command CS2-514
  - privilege level (global) command CS2-253
  - privilege level (line) command CS2-253, CS2-255
  - profile incoming command CS2-515
  - protocol (ATM) command CS2-33
  - protocol (VPDN) command CS2-516
  - protocol rlm port command CS2-515
  - pulse-time command CS2-343
  - pvc command CS2-35
  - pvc-in-range command CS2-54
- 
- Q**
- query url command CS2-240
- 
- R**
- radius-server attribute 188 format command CS2-175
  - radius-server attribute 32 include-in-access-req command CS2-174
  - radius-server attribute 44 include-in-access-req command CS2-175
  - radius-server attribute 69 clear command CS2-175

radius-server attribute 8 include-in-access-req command CS2-174

radius-server attribute nas-port format command CS2-176

radius-server configure-nas command CS2-176

radius-server deadtime command CS2-177

radius-server directed-request command CS2-177

radius-server extended-portnames command CS2-177

radius-server host command CS2-177

radius-server host non-standard command CS2-178

radius-server key command CS2-179

radius-server optional passwords command CS2-179

radius-server retransmit command CS2-179

radius-server timeout 8 command CS2-180

radius-server vsa send command CS2-180

range command CS2-516

range pvc command CS2-55

rate-limit command CS2-704

rcapi number command CS2-517

rcapi server command CS2-517

rd command CS2-705

reload command CS2-517

reload components command CS2-518

request dialin command CS2-518

request dialout command CS2-519

resource command CS2-519

resource-pool aaa accounting ppp command CS2-520

resource-pool aaa protocol command CS2-520

resource-pool call treatment command CS2-520

resource-pool call treatment discriminator command CS2-521

resource-pool command CS2-519

resource-pool group resource command CS2-521

resource-pool profile customer command CS2-521

resource-pool profile discriminator command CS2-522

resource-pool profile service command CS2-522

resource-pool profile vpdn command CS2-522

resume (setting X.3 parameters) command CS2-609

resume (switching sessions) command CS2-612

retry keepalive command CS2-523

ring-speed command CS2-343

rlogin command CS2-613

rlogin trusted-localuser-source command CS2-613

rlogin trusted-remoteuser-source local command CS2-613

root CEP command CS2-240

root PROXY command CS2-241

root TFTP command CS2-241

rotary command CS2-523

rotary-group command CS2-523

route-target command CS2-705

---

## S

scramble command CS2-343

scrambling cell-payload command CS2-36

scrambling-payload command CS2-36

script activation command CS2-524

script arap-callback command CS2-524

script callback command CS2-524

script connection command CS2-525

script dialer command CS2-525

script reset command CS2-525

script startup command CS2-526

sdhc cts-delay command

*See half-duplex timer command*

sdhc hdx command

*See half-duplex command*

sdhc rts-delay command

*See half-duplex timer command*

server (RADIUS) command CS2-180

server (RLM) command CS2-526

server (TACACS+) command CS2-184

service exec-callback command CS2-614

service module t1 fdl command CS2-347

service old-slip-prompts command CS2-614

service pad command CS2-105

service pad from-xot command CS2-106

service pad to-xot command CS2-106

service password-encryption command CS2-255

- service pt-vty-logging command CS2-614
- service single-slot-reload-enable command CS2-352
- service translation command CS2-93
- service-module 56k clock rate command CS2-344
- service-module 56k clock source command CS2-345
- service-module 56k data-coding command CS2-345
- service-module 56k network-type command CS2-345
- service-module 56k remote-loopback command CS2-346
- service-module 56k switched-carrier command CS2-346
- service-module t1 clock source command CS2-346
- service-module t1 data-coding command CS2-347
- service-module t1 framing command CS2-347
- service-module t1 lbo command CS2-348
- service-module t1 linecode command CS2-348
- service-module t1 remote-alarm-enable command CS2-348
- service-module t1 remote-loopback command CS2-349
- service-module t1 timeslots command CS2-351
- session-limit command CS2-615
- session-timeout command CS2-615
- set ip next-hop verify-availability command CS2-706
- set mpls experimental command CS2-706
- set ospf router-id command CS2-706
- set peer (IPSec) command CS2-229
- set peer command CS2-229
- set pfs command CS2-229
- set security-association level per-host command CS2-229
- set security-association lifetime command CS2-230
- set session-key command CS2-230
- set transform-set command CS2-231
- sgbp dial-bids command CS2-526
- sgbp group command CS2-527
- sgbp member command CS2-527
- sgbp ppp-forward command CS2-527
- sgbp seed-bid command CS2-528
- shelf-id command CS2-528
- shortcut-frame-count command CS2-707
- shortcut-frame-time command CS2-707
- show accounting command CS2-167
- show adjacency command CS2-707
- show aps command CS2-352
- show arap command CS2-615
- show async status command CS2-529
- show atm arp-server command CS2-37
- show atm class-links command CS2-37
- show atm interface atm command CS2-38
- show atm map command CS2-38
- show atm pvc command CS2-39
- show atm svc command CS2-39
- show atm svc ppp command CS2-55
- show atm traffic command CS2-40
- show atm vc command CS2-40
- show atm vc privileged command CS2-707
- show atm vp command CS2-41
- show busyout command CS2-529
- show cable bundle command CS2-708
- show call calltracker active command CS2-530
- show call calltracker handle command CS2-530
- show call calltracker history command CS2-530
- show call calltracker summary command CS2-530
- show call progress tone command CS2-531
- show caller command CS2-531
- show cef command CS2-708
- show cef interface command CS2-708
- show cef linecard command CS2-708
- show ces circuit command CS2-42
- show ces command CS2-41
- show ces interface cbr command CS2-42
- show ces status command CS2-42
- show cmns command CS2-106
- show compress command CS2-352
- show connect command CS2-94
- show controllers atm command CS2-42
- show controllers bri command CS2-532
- show controllers cbus command CS2-352
- show controllers e1 call-counters command CS2-533
- show controllers e1 cas-data command CS2-533
- show controllers e1 command CS2-533

show controllers ethernet command CS2-353  
show controllers fastethernet command CS2-353  
show controllers fddi command CS2-354  
show controllers gigabitethernet command CS2-354  
show controllers lex command CS2-354  
show controllers mci command CS2-355  
show controllers pibus command CS2-355  
show controllers pos command CS2-355  
show controllers serial command CS2-356  
show controllers t1 bert command CS2-357  
show controllers t1 call-counters command CS2-534  
show controllers t1 cas-data command CS2-534  
show controllers t1 command CS2-356  
show controllers t1 timeslots command CS2-534  
show controllers t3 command CS2-357  
show controllers token command CS2-358  
show controllers vg-anylan command CS2-358  
show controllers vsi control-interface command CS2-709  
show controllers vsi descriptor command CS2-709  
show controllers vsi session command CS2-709  
show controllers vsi status command CS2-710  
show controllers vsi traffic command CS2-710  
show controllers XTagATM command CS2-710  
show cot dsp command CS2-535  
show cot request command CS2-535  
show cot summary command CS2-536  
show crypto ca certificates command CS2-241  
show crypto ca roots command CS2-241  
show crypto dynamic-map command CS2-231  
show crypto ipsec sa command CS2-232  
show crypto ipsec security-association lifetime command CS2-232  
show crypto ipsec transform-set command CS2-232  
show crypto isakmp policy command CS2-250  
show crypto isakmp sa command CS2-250  
show crypto key mypubkey rsa command CS2-250  
show crypto key pubkey-chain rsa command CS2-250  
show crypto map (IPSec) command CS2-233  
show dhcp command CS2-536  
show diag command CS2-358  
show diagbus command CS2-359  
show dialer command CS2-536  
show dialer dnis command CS2-537  
show dialer interface bri command CS2-537  
show dialer map command CS2-537  
show dialer sessions command CS2-537  
show dial-shelf command CS2-538  
show dial-shelf split command CS2-538  
show dnsix command CS2-266  
show dsc clock command CS2-538  
show dsi command CS2-538  
show dsip clients command CS2-539  
show dsip command CS2-539  
show dsip nodes command CS2-539  
show dsip ports command CS2-539  
show dsip queue command CS2-540  
show dsip tracing command CS2-540  
show dsip transport command CS2-540  
show dsip version command CS2-540  
show dxi map command CS2-43  
show dxi pvc command CS2-43  
show entry command CS2-615  
show frame-relay end-to-end keepalive command CS2-86  
show frame-relay ip tcp header-compression command CS2-86  
show frame-relay lapf command CS2-87  
show frame-relay lmi command CS2-87  
show frame-relay map command CS2-87  
show frame-relay pvc command CS2-87  
show frame-relay qos-autosense command CS2-88  
show frame-relay route command CS2-88  
show frame-relay svc maplist command CS2-88  
show frame-relay traffic command CS2-88  
show hub command CS2-359  
show ima interface atm command CS2-44  
show interface cbr command CS2-44  
show interface stats command CS2-710  
show interface XTagATM command CS2-711

- show interfaces atm command CS2-45
- show interfaces bri command CS2-541
- show interfaces command CS2-359
- show interfaces ctunnel command CS2-360
- show interfaces ethernet accounting command CS2-361
- show interfaces ethernet command CS2-361
- show interfaces fastethernet command CS2-361
- show interfaces fddi accounting command CS2-362
- show interfaces fddi command CS2-362
- show interfaces gigabitethernet command CS2-362
- show interfaces hssi command CS2-363
- show interfaces ip-brief command CS2-363
- show interfaces lex command CS2-363
- show interfaces loopback command CS2-364
- show interfaces port-channel command CS2-364
- show interfaces pos command CS2-364
- show interfaces serial accounting command CS2-365
- show interfaces serial bchannel command CS2-541
- show interfaces serial command CS2-365
- show interfaces tokenring command CS2-366
- show interfaces tunnel command CS2-367
- show interfaces vg-anylan command CS2-367
- show interfaces virtual-access command CS2-542
- show ip audit configuration command CS2-216
- show ip audit interface command CS2-217
- show ip audit statistics command CS2-217
- show ip auth-proxy command CS2-221
- show ip bgp vpnv4 command CS2-711
- show ip cache command CS2-712
- show ip cache flow aggregation command CS2-713
- show ip cache flow command CS2-713
- show ip cef command CS2-713
- show ip cef vrf command CS2-714
- show ip director dfp command CS2-367
- show ip explicit-paths command CS2-715
- show ip flow export command CS2-715
- show ip inspect command CS2-210
- show ip interface virtual-access command CS2-542
- show ip local-pool command CS2-542
- show ip mcache command CS2-715
- show ip mds forwarding command CS2-716
- show ip mds interface command CS2-716
- show ip mds stats command CS2-716
- show ip mds summary command CS2-716
- show ip mroute command CS2-717
- show ip ospf database opaque-area command CS2-717
- show ip ospf mpls traffic-eng command CS2-717
- show ip pim interface command CS2-718
- show ip port-map command CS2-224
- show ip protocols vrf command CS2-718
- show ip route command CS2-542
- show ip route vrf command CS2-718
- show ip rsvp host command CS2-719
- show ip ssh command CS2-270
- show ip traffic-engineering command CS2-719
- show ip traffic-engineering configuration command CS2-719
- show ip traffic-engineering routes command CS2-720
- show ip trigger-authentication command CS2-153
- show ip vrf command CS2-720
- show ipx compression command CS2-543
- show ipx spx-protocol command CS2-543
- show isdn command CS2-544
- show isdn nfas group command CS2-544
- show isdn service command CS2-545
- show isdn status command CS2-465
- show isis database verbose command CS2-720
- show isis mpls traffic-eng adjacency-log command CS2-721
- show isis mpls traffic-eng advertisements command CS2-721
- show isis mpls traffic-eng tunnel command CS2-721
- show kerberos creds command CS2-191
- show keymap command CS2-616
- show lane bus command CS2-722
- show lane client command CS2-723
- show lane command CS2-721
- show lane config command CS2-724
- show lane database command CS2-724

- show lane default-atm-addresses command CS2-724
- show lane le-arp command CS2-725
- show lane server command CS2-726
- show lat advertised command CS2-616
- show lat groups command CS2-616
- show lat nodes command CS2-616
- show lat services command CS2-617
- show lat sessions command CS2-617
- show lat traffic command CS2-617
- show line async-queue command CS2-545
- show line command CS2-617
- show mls rp command CS2-727
- show mls rp interface command CS2-727
- show mls rp ip multicast command CS2-727
- show mls rp ipx command CS2-728
- show mls rp vtp-domain command CS2-728
- show modem at-mode command CS2-545
- show modem call-stats command CS2-546
- show modem calltracker command CS2-546
- show modem command CS2-545
- show modem configuration command CS2-546
- show modem connect-speeds command CS2-546
- show modem cookie command CS2-547
- show modem csm command CS2-547
- show modem log command CS2-547
- show modem mapping command CS2-548
- show modem mica command CS2-548
- show modem operational-status command CS2-548
- show modem summary command CS2-549
- show modem test command CS2-549
- show modem version command CS2-549
- show modemcap command CS2-549
- show modem-pool command CS2-548
- show mpls forwarding-table command CS2-728
- show mpls interfaces command CS2-729
- show mpls label range command CS2-729
- show mpls traffic-eng autoroute command CS2-729
- show mpls traffic-eng link-management admission-control command CS2-730
- show mpls traffic-eng link-management advertisements command CS2-730
- show mpls traffic-eng link-management bandwidth-allocation command CS2-730
- show mpls traffic-eng link-management igp-neighbors command CS2-730
- show mpls traffic-eng link-management interfaces command CS2-731
- show mpls traffic-eng link-management summary command CS2-731
- show mpls traffic-eng topology command CS2-731
- show mpls traffic-eng topology path command CS2-732
- show mpls traffic-eng tunnels command CS2-732
- show mpls traffic-eng tunnels summary command CS2-733
- show mpoa client cache command CS2-734
- show mpoa client command CS2-734
- show mpoa client statistics command CS2-734
- show mpoa default-atm-addresses command CS2-734
- show mpoa server cache command CS2-735
- show mpoa server command CS2-735
- show mpoa server statistics command CS2-735
- show nbf cache command CS2-550
- show nbf sessions command CS2-550
- show network-clocks command CS2-45
- show node command CS2-618
- show pas caim command CS2-368
- show pas eswitch address command CS2-368
- show pci aim command CS2-368
- show port config command CS2-550
- show port digital log command CS2-551
- show port modem calltracker command CS2-551
- show port modem log command CS2-552
- show port modem test command CS2-552
- show port operational-status command CS2-553
- show ppp bap command CS2-553
- show ppp mppe command CS2-553
- show ppp multilink command CS2-554
- show ppp queues command CS2-153
- show privilege command CS2-255

show pxf accounting command CS2-735  
show pxf crash command CS2-736  
show pxf feature cef command CS2-736  
show pxf feature nat command CS2-736  
show pxf interface command CS2-736  
show queuing virtual-access command CS2-554  
show radius statistics command CS2-181  
show rcapi status command CS2-554  
show redundancy command CS2-554  
show redundancy history command CS2-554  
show resource-pool call command CS2-555  
show resource-pool customer command CS2-555  
show resource-pool discriminator command CS2-555  
show resource-pool resource command CS2-555  
show resource-pool vpdn command CS2-556  
show rlm group statistics command CS2-556  
show rlm group status command CS2-556  
show rlm group timer command CS2-556  
show route-map ipc command CS2-737  
show running map-class command CS2-89  
show service command CS2-618  
show service-module serial command CS2-369  
show sessions command CS2-557  
show sgbp command CS2-557  
show sgbp queries command CS2-557  
show smds addresses command CS2-96  
show smds map command CS2-96  
show smds traffic command CS2-96  
show smf command CS2-369  
show snapshot command CS2-558  
show sntp command CS2-369  
show spe command CS2-558  
show spe digital active command CS2-559  
show spe digital command CS2-558  
show spe digital csr command CS2-559  
show spe digital disconnect-reason command CS2-560  
show spe digital summary command CS2-560  
show spe log command CS2-560  
show spe modem active command CS2-561  
show spe modem command CS2-561  
show spe modem csr command CS2-562  
show spe modem disconnect-reason command CS2-562  
show spe modem high speed command CS2-563  
show spe modem high standard command CS2-563  
show spe modem low speed command CS2-564  
show spe modem low standard command CS2-564  
show spe modem summary command CS2-565  
show spe recovery command CS2-565  
show spe version command CS2-566  
show sscop command CS2-45  
show ssh command CS2-270  
show tag-switching atm-tdp bindings command CS2-737  
show tag-switching atm-tdp bindwait command CS2-737  
show tag-switching atm-tdp capability command CS2-737  
show tag-switching atm-tdp summary command CS2-738  
show tag-switching cos-map command CS2-738  
show tag-switching forwarding vrf command CS2-739  
show tag-switching forwarding-table command CS2-738  
show tag-switching interfaces command CS2-739  
show tag-switching prefix-map command CS2-739  
show tag-switching tdp bindings command CS2-740  
show tag-switching tdp discovery command CS2-740  
show tag-switching tdp neighbors command CS2-740  
show tag-switching tdp parameters command CS2-741  
show tag-switching tsp-tunnels command CS2-741  
show tcp intercept connections command CS2-202  
show tcp intercept statistics command CS2-202  
show tdm backplane command CS2-369  
show tdm connections command CS2-370  
show tdm data command CS2-371  
show tdm detail command CS2-372  
show tdm information command CS2-372  
show tdm pool command CS2-373  
show terminal command CS2-618  
show tgrm command CS2-566  
show tn3270 ascii-hexval command CS2-618  
show tn3270 character-map command CS2-619  
show translate command CS2-619

show ttycap command CS2-619  
show users command CS2-619  
show vc-group command CS2-94  
show vlans command CS2-741  
show vpdn command CS2-567  
show vpdn domain command CS2-567  
show vpdn group command CS2-567  
show vpdn history failure command CS2-568  
show vpdn multilink command CS2-568  
show x25 context command CS2-106  
show x25 cug command CS2-107  
show x25 hunt-group command CS2-107  
show x25 interface command CS2-107  
show x25 map command CS2-107  
show x25 pad command CS2-620  
show x25 profile command CS2-108  
show x25 remote-red command CS2-108  
show x25 route command CS2-108  
show x25 services command CS2-108  
show x25 vc command CS2-108  
show x25 xot command CS2-109  
show xremote command CS2-620  
show xremote line command CS2-620  
show xtagatm cos-bandwidth-allocation XTagATM  
command CS2-742  
show xtagatm cross-connect command CS2-742  
show xtagatm vc command CS2-742  
shutdown (controller) command CS2-373  
shutdown (hub) command CS2-373  
shutdown (interface) command CS2-374  
shutdown (port) command CS2-568  
shutdown (PVC range) command CS2-56  
shutdown (PVC-in-range) command CS2-55  
shutdown (RLM) command CS2-568  
shutdown (spe) command CS2-569  
shutdown command CS2-94  
signaling-class cas command CS2-569  
slip command CS2-621  
smds address command CS2-97  
smds dxi command CS2-97  
smds enable-arp command CS2-97  
smds glean command CS2-98  
smds multicast arp command CS2-98  
smds multicast bridge command CS2-99  
smds multicast command CS2-98  
smds multicast ip command CS2-99  
smds static-map command CS2-99  
smt-queue-threshold command CS2-374  
snapshot client command CS2-569  
snapshot server command CS2-570  
snmp ifindex clear command CS2-374  
snmp ifindex persist command CS2-375  
snmp trap illegal-address command CS2-375  
source template command CS2-570  
source-address command CS2-376  
source-ip command CS2-570  
spe call-record command CS2-571  
spe command CS2-571  
spe country command CS2-571  
spe download maintenance command CS2-573  
spe log-event-size command CS2-573  
spe recovery command CS2-573  
speed command CS2-376  
squelch command CS2-376  
srp loopback command CS2-377  
srp priority-map command CS2-378  
srp random-detect command CS2-378  
srp shutdown command CS2-378  
srp tx-traffic-rate command CS2-379  
srp-deficit-round-robin command CS2-377  
sscop cc-timer command CS2-46  
sscop keepalive-timer command CS2-46  
sscop max-cc command CS2-46  
sscop poll-timer command CS2-47  
sscop receive-window command CS2-47  
sscop send-window command CS2-47  
ssh command CS2-270  
ssrp buffer-size command CS2-377

start-character command CS2-574  
 start-chat command CS2-574  
 stop-character command CS2-575  
 svc command CS2-47

---

**T**

t1 bert command CS2-379  
 t1 clock source command CS2-380  
 t1 command CS2-379  
 t1 external command CS2-380  
 t1 fdl ansi command CS2-380  
 t1 framing command CS2-381  
 t1 linecode command CS2-381  
 t1 test command CS2-381  
 t1 timeslot command CS2-382  
 t1 yellow command CS2-382  
 tacacs-server directed-request command CS2-184  
 tacacs-server host command CS2-184  
 tacacs-server key command CS2-185  
 tag-control-protocol vsi command CS2-743  
 tag-switching advertise-tags command CS2-743  
 tag-switching atm allocation-mode command CS2-744  
 tag-switching atm control-vc interface configuration command CS2-744  
 tag-switching atm maxhops command CS2-745  
 tag-switching atm vc-merge command CS2-746  
 tag-switching atm vpi command CS2-746  
 tag-switching atm vp-tunnel command CS2-746  
 tag-switching cos-map command CS2-746  
 tag-switching ip (global configuration) command CS2-747  
 tag-switching ip (interface configuration) command CS2-747  
 tag-switching ip default-route command CS2-747  
 tag-switching mtu command CS2-747  
 tag-switching prefix-map command CS2-748  
 tag-switching request-tags for command CS2-748  
 tag-switching tag-range downstream command CS2-748  
 tag-switching tdp discovery command CS2-749  
 tag-switching tdp holdtime command CS2-749  
 tag-switching tsp-tunnels (global configuration) command CS2-749  
 tag-switching tsp-tunnels (interface configuration) command CS2-750  
 telnet break-on-ip command CS2-623  
 telnet command CS2-622  
 telnet refuse-negotiations command CS2-624  
 telnet speed command CS2-624  
 telnet sync-on-break command CS2-624  
 telnet transparent command CS2-625  
 template command CS2-575  
 terminal lat out-group command CS2-625  
 terminal lat remote-modification command CS2-625  
 terminal transport preferred command CS2-625  
 terminate-from command CS2-575  
 test aim eeprom command CS2-382  
 test interface fastethernet command CS2-383  
 test modem back-to-back command CS2-576  
 test port modem back-to-back command CS2-576  
 test service-module command CS2-383  
 threshold de command CS2-89  
 threshold ecn command CS2-89  
 timeout login response command CS2-154  
 timeslot command CS2-383  
 tn3270 8bit display command CS2-626  
 tn3270 8bit transparent-mode command CS2-627  
 tn3270 character-map command CS2-627  
 tn3270 command CS2-626  
 tn3270 datastream command CS2-627  
 tn3270 null-processing command CS2-628  
 tn3270 optimize-cursor-move command CS2-628  
 tn3270 reset-required command CS2-628  
 tn3270 status-message command CS2-629  
 tn3270 typeahead command CS2-629  
 traffic-engineering filter command CS2-750  
 traffic-engineering route command CS2-750  
 translate lat (virtual access interfaces) command CS2-633  
 translate lat command CS2-629

translate tcp (virtual access interfaces) command CS2-637  
translate tcp command CS2-634  
translate x25 (virtual access interfaces) command CS2-644  
translate x25 command CS2-639  
transmit-buffers backing-store command CS2-384  
transmit-clock-internal command CS2-384  
transmitter-delay command CS2-384  
transport input command CS2-646  
transport output command CS2-647  
transport preferred command CS2-647  
trunk group (global) command CS2-577  
trunkgroup (dial-peer) command CS2-578  
trunk-group (interface) command CS2-578  
ts16 command CS2-385  
ttycap command CS2-648  
tunnel checksum command CS2-385  
tunnel command CS2-578  
tunnel destination command CS2-385  
tunnel key command CS2-386  
tunnel mode command CS2-386  
tunnel mode mpls traffic-eng command CS2-751  
tunnel mode tag-switching command CS2-751  
tunnel mpls traffic-eng affinity command CS2-751  
tunnel mpls traffic-eng autoroute announce command CS2-752  
tunnel mpls traffic-eng autoroute metric command CS2-752  
tunnel mpls traffic-eng bandwidth command CS2-752  
tunnel mpls traffic-eng path-option command CS2-753  
tunnel mpls traffic-eng priority command CS2-753  
tunnel sequence-datagrams command CS2-386  
tunnel source command CS2-387  
tunnel tsp-hop command CS2-754  
tx-queue-limit command CS2-387  
txspeed command CS2-648

---

## U

ubr command CS2-48  
ubr+ command CS2-48  
username command CS2-255

---

## V

vbr-nrt command CS2-49  
vc-group command CS2-94  
virtual-profile aaa command CS2-578  
virtual-profile if-needed command CS2-579  
virtual-profile virtual-template command CS2-579  
virtual-template command CS2-579  
vpdn aaa attribute command CS2-579  
vpdn aaa attribute nas-port vpdn-nas command CS2-181  
vpdn aaa override-server command CS2-580  
vpdn domain-delimiter command CS2-580  
vpdn enable command CS2-580  
vpdn group command CS2-581  
vpdn history failure table-size command CS2-581  
vpdn logging command CS2-581  
vpdn logging history failure command CS2-582  
vpdn profile command CS2-582  
vpdn search-order command CS2-582  
vpdn session-limit command CS2-583  
vpdn softshut command CS2-583  
vpdn source-ip command CS2-583  
vty-async command CS2-584  
vty-async dynamic-routing command CS2-584  
vty-async header-compression command CS2-584  
vty-async ipx ppp-client loopback command CS2-585  
vty-async keepalive command CS2-585  
vty-async mtu command CS2-585  
vty-async ppp authentication command CS2-586  
vty-async ppp use-tacacs command CS2-586  
vty-async virtual-template command CS2-586

**W**

where command CS2-648

**X**

x25 accept-reverse command CS2-109

x25 address command CS2-109

x25 alias command CS2-109

x25 aodi command CS2-587

x25 bfe-decision command CS2-110

x25 bfe-emergency command CS2-110

x25 default command CS2-110

x25 facility command CS2-110

x25 failover command CS2-111

x25 hic command CS2-111

x25 hoc command CS2-111

x25 hold-queue command CS2-112

x25 hold-vc-timer command CS2-112

x25 host command CS2-112

x25 htc command CS2-113

x25 hunt-group command CS2-113

x25 idle command CS2-113

x25 ip-precedence command CS2-113

x25 ips command CS2-114

x25 lic command CS2-114

x25 linkrestart command CS2-114

x25 loc command CS2-114

x25 ltc command CS2-115

x25 map bridge command CS2-118

x25 map emns command CS2-118

x25 map command CS2-115

x25 map compressedtcp command CS2-119

x25 map pad command CS2-119

x25 map ppp command CS2-587

x25 modulo command CS2-119

x25 nvc command CS2-120

x25 ops command CS2-120

x25 pad-access command CS2-120

x25 profile command CS2-120

x25 pvc (encapsulating) command CS2-121

x25 pvc (switched PVC to SVC) command CS2-123

x25 pvc (switched) command CS2-122

x25 pvc (XOT) command CS2-124

x25 remote-red command CS2-125

x25 retry command CS2-125

x25 roa command CS2-126

x25 route command CS2-126

x25 routing acknowledge local command CS2-130

x25 routing command CS2-130

x25 subaddress command CS2-649

x25 subscribe cug-service command CS2-130

x25 subscribe flow-control command CS2-131

x25 subscribe local-cug command CS2-131

x25 subscribe packetsize command CS2-132

x25 subscribe windowsize command CS2-132

x25 suppress-called-address command CS2-132

x25 suppress-calling-address command CS2-133

x25 t10 command CS2-133

x25 t11 command CS2-133

x25 t12 command CS2-133

x25 t13 command CS2-134

x25 t20 command CS2-134

x25 t21 command CS2-134

x25 t22 command CS2-134

x25 t23 command CS2-135

x25 threshold command CS2-135

x25 use-source-address command CS2-135

x25 win command CS2-135

x25 wout command CS2-136

x28 command CS2-649

x29 access-list command CS2-136

x29 profile command CS2-136

x3 command CS2-650

xremote command CS2-650

xremote lat command CS2-650

xremote tftp buffersize command CS2-650

xremote tftp host command CS2-651

xremote tftp retries command CS2-651

xremote xdm command CS2-651

---

## **Y**

yellow command CS2-387