

## **Cisco IOS Command Summary Volume 3 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-7813361=  
Text Part Number: 78-13361-01

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.

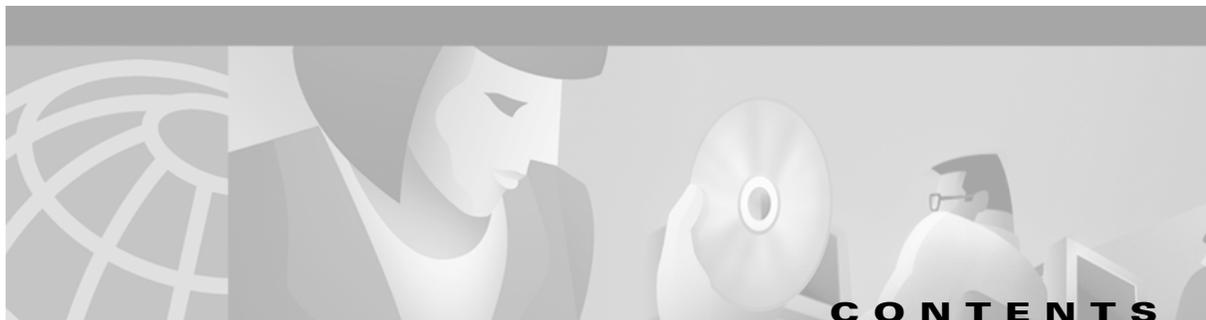
AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ 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 3 of 3*

Copyright © 2001, Cisco Systems, Inc.

All rights reserved.



**About Cisco IOS Software Documentation** v

**Using Cisco IOS Software** xv

---

**Bridging and IBM Networking**  
**Volume 1 of 2**

**Transparent Bridging Commands** CS3-3

**Source-Route Bridging Commands** CS3-27

**Token Ring Inter-Switch Link Commands** CS3-55

**Token Ring Route Switch Module Commands** CS3-57

**Remote Source-Route Bridging Commands** CS3-59

**DLSw+ Commands** CS3-67

**Serial Tunnel and Block Serial Tunnel Commands** CS3-95

**LLC2 and SDLC Commands** CS3-115

**IBM Network Media Translation Commands** CS3-131

**SNA Frame Relay Access Support Commands** CS3-141

**NCIA Client/Server Commands** CS3-147

**Airline Product Set Commands** CS3-151

---

**Bridging and IBM Networking**  
**Volume 2 of 2**

**DSPU and SNA Service Point Commands CS3-171**

**SNA Switching Services Commands CS3-193**

**Cisco Transaction Connection Commands CS3-213**

**Cisco Mainframe Channel Connection Commands CS3-229**

**CLAW and TCP/IP Offload Commands CS3-239**

**CMPC, CMPC+, and CSNA Commands CS3-245**

**TN3270 Server Commands CS3-251**

---

**Quality of Service Solutions**

**Quality of Service Commands: access-list rate-limit Through match ip dscp CS3-277**

**Quality of Service Commands: match ip precedence Through set qos-group CS3-301**

**Quality of Service Commands: shape Through vc-hold-queue CS3-325**

---

**Voice, Video, and Fax**

**Voice, Video, and Fax Commands: acc-qos Through customer-id CS3-343**

**Voice, Video, and Fax Commands: default Through ftc-trunk management-protocol CS3-393**

**Voice, Video, and Fax Commands: gatekeeper Through proxy h323 CS3-425**

**Voice, Video, and Fax Commands: register e164 Through shutdown (voice-port) CS3-475**

**Voice, Video, and Fax Commands: signal Through zone subnet CS3-521**

---

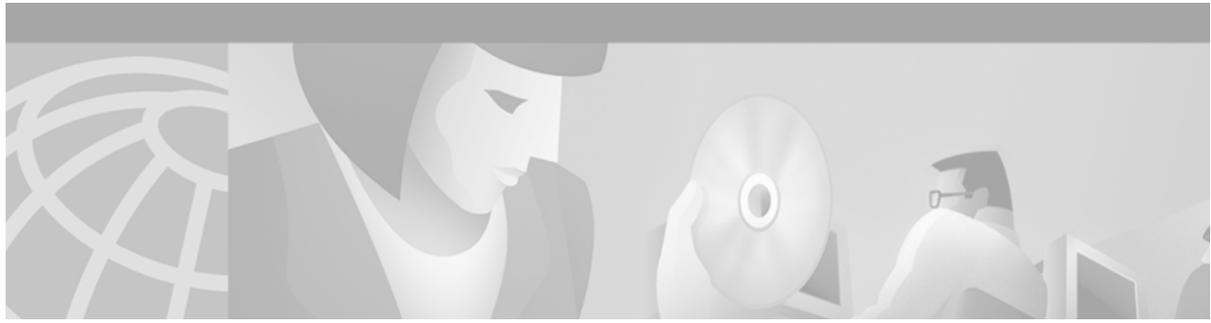
**Mobile Wireless**

**Mobile Wireless Commands CS3-569**

**SGSN D-Node Commands CS3-589**

---

**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.

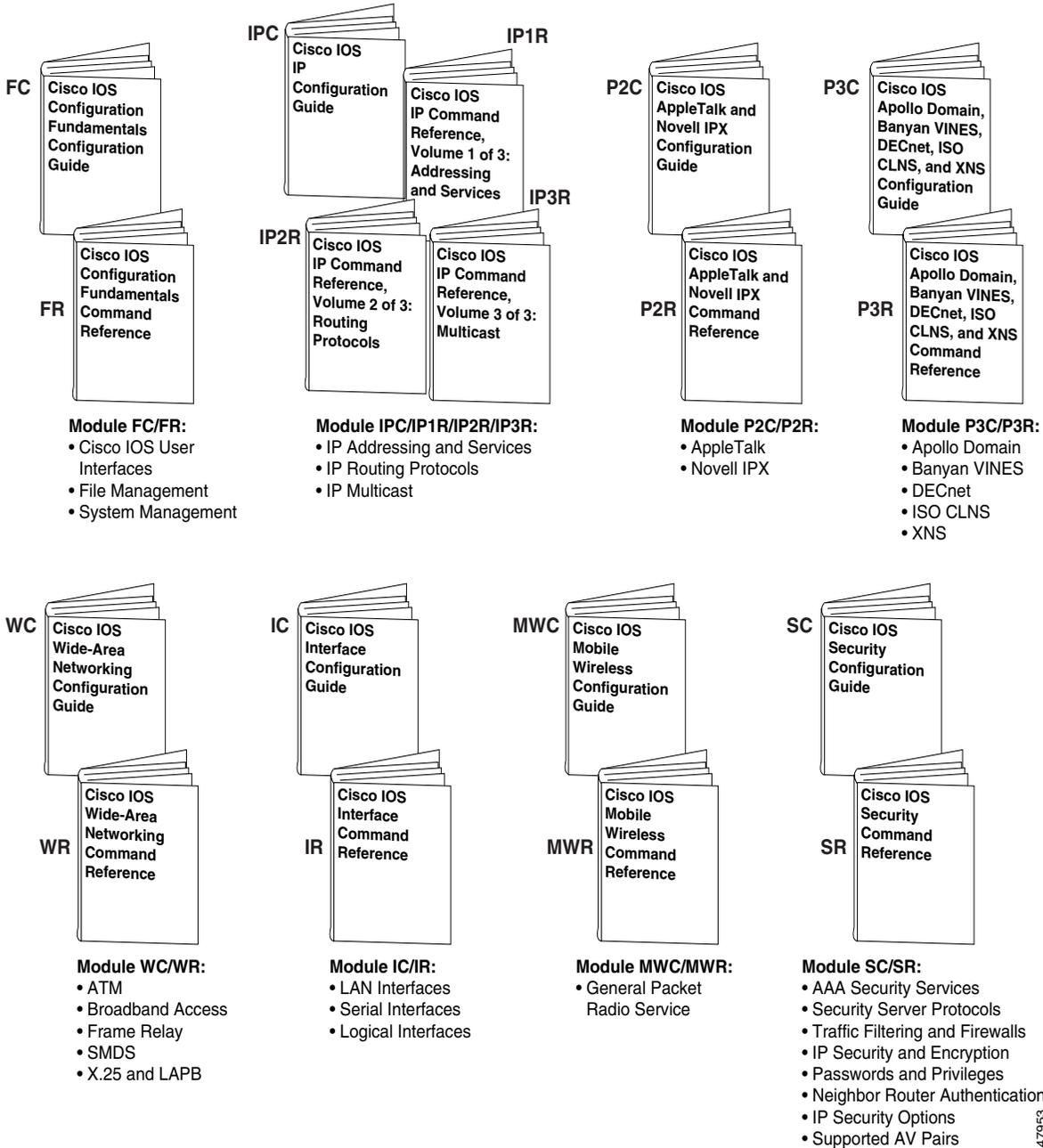
Figure 1 shows the Cisco IOS software documentation modules.



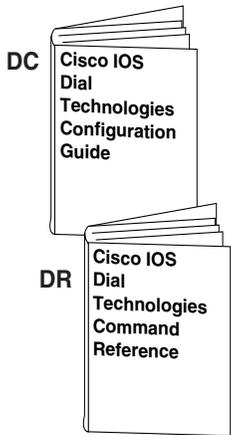
**Note**

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**

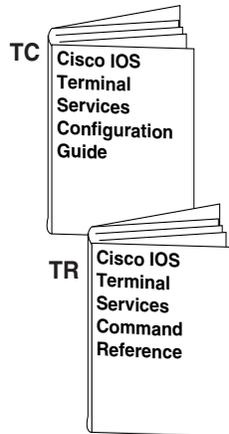


47953



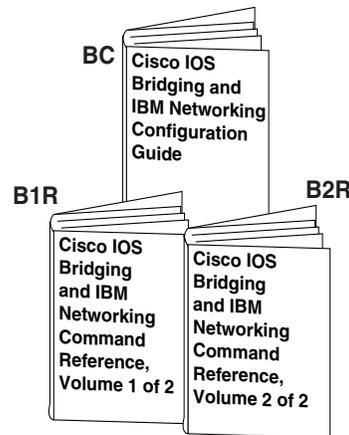
**Module DC/DR:**

- 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

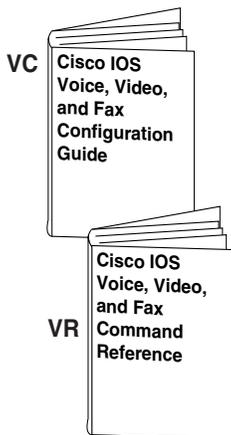


**Module BC/B1R:**

- 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

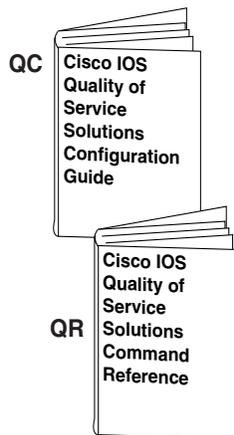
**Module BC/B2R:**

- 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



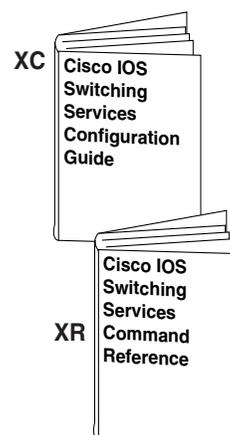
**Module VC/VR:**

- 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* (two 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</i> <Tab>	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>

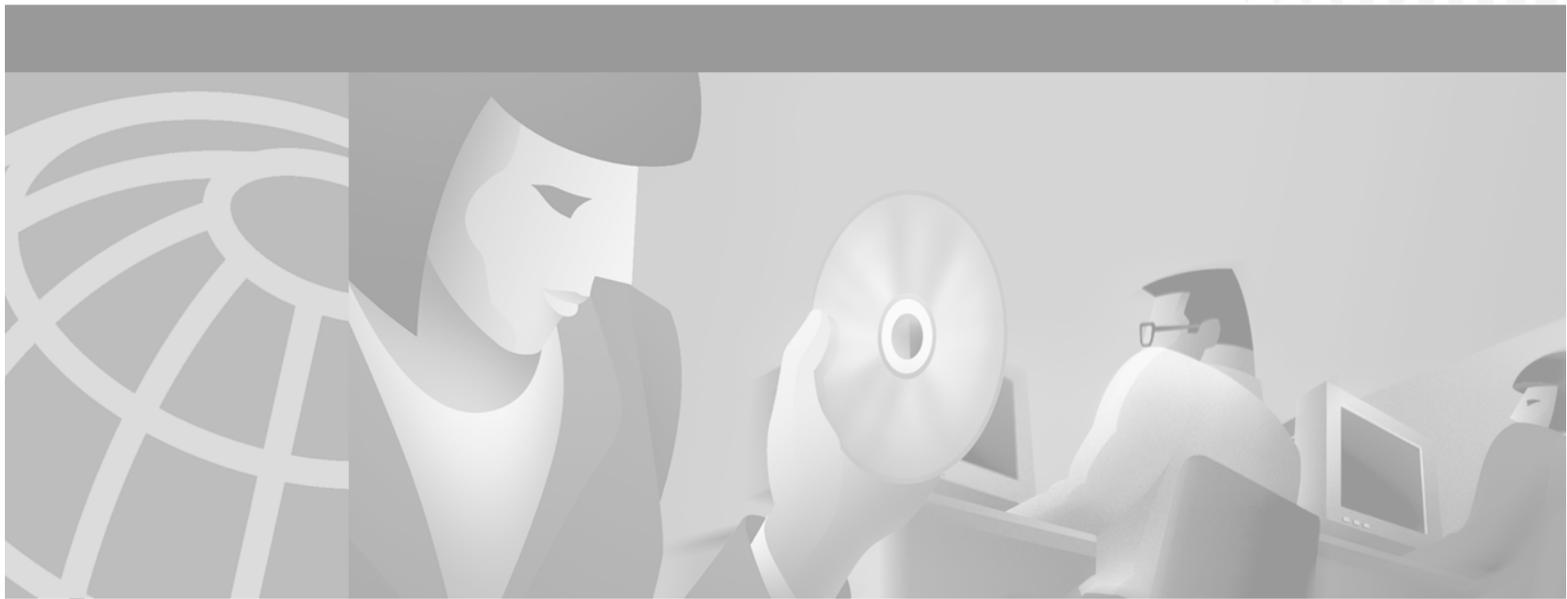
## Using Software Release Notes

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.





**Bridging and IBM Networking  
Volume 1 of 2**





## Transparent Bridging Commands

This chapter describes the function and syntax of the transparent bridging commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### access-list (extended-ibm)

To provide extended access lists that allow more detailed access lists, use the **access-list** global configuration command. These lists allow you to specify both source and destination addresses and arbitrary bytes in the packet.

```
access-list access-list-number {permit | deny} source source-mask destination destination-mask offset size operator operand
```

Syntax Description		
	<i>access-list-number</i>	Integer from 1100 to 1199 that you assign to identify one or more <b>permit/deny</b> conditions as an extended access list. Note that a list number in the range 1100 to 1199 distinguishes an extended access list from other access lists.
	<b>permit</b>	Allows a connection when a packet matches an access condition. The Cisco IOS software stops checking the extended access list after a match occurs. All conditions must be met to make a match.
	<b>deny</b>	Disallows a connection when a packet matches an access condition. The software stops checking the extended access list after a match occurs. All conditions must be met to make a match.
	<i>source</i>	MAC Ethernet address in the form <i>xxxx.xxxx.xxxx</i> .
	<i>source-mask</i>	Mask of MAC Ethernet source address bits to be ignored. The software uses the <i>source</i> and <i>source-mask</i> arguments to match the source address of a packet.
	<i>destination</i>	MAC Ethernet value used for matching the destination address of a packet.
	<i>destination-mask</i>	Mask of MAC Ethernet destination address bits to be ignored. The software uses the <i>destination</i> and <i>destination mask</i> arguments to match the destination address of a packet.

<i>offset</i>	Range of values that must be satisfied in the access list. Specified in decimal or in hexadecimal format in the form <i>0xnn</i> . The offset is the number of bytes from the destination address field; it is not an offset from the start of the packet. The number of bytes you need to offset from the destination address varies depending on the media encapsulation type you are using.
<i>size</i>	Range of values that must be satisfied in the access list. Must be an integer 1 to 4.
<i>operator</i>	Compares arbitrary bytes within the packet. Can be one of the following keywords: <b>lt</b> —less than <b>gt</b> —greater than <b>eq</b> —equal <b>neq</b> —not equal <b>and</b> —bitwise and <b>xor</b> —bitwise exclusive or <b>nop</b> —address match only
<i>operand</i>	Compares arbitrary bytes within the packet. The value to be compared to or masked against.

## access-list (standard-ibm)

To establish a MAC address access lists, use the **access-list** global configuration command. To remove a single access-list entry, use the **no** form of this command.

**access-list** *access-list-number* {**permit** | **deny**} *address mask*

**no access-list** *access-list-number*

### Syntax Description

<i>access-list-number</i>	Integer from 700 to 799 that you select for the list.
<b>permit</b>	Permits the frame.
<b>deny</b>	Denies the frame.
<i>address mask</i>	48-bit MAC addresses written as a dotted triple of four-digit hexadecimal numbers. The ones bits in the <i>mask</i> argument are the bits to be ignored in <i>address</i> .

## access-list (type-code-ibm)

To build type-code access lists, use the **access-list** global configuration command. To remove a single access list entry, use the **no** form of this command.

**access-list** *access-list-number* {**permit** | **deny**} *type-code wild-mask*

**no access-list** *access-list-number*

<b>Syntax Description</b>	<i>access-list-number</i>	User-selectable number between 200 and 299 that identifies the list.
	<b>permit</b>	Permits the frame.
	<b>deny</b>	Denies the frame.
	<i>type-code</i>	16-bit hexadecimal number written with a leading "0x"; for example, 0x6000. You can specify either an Ethernet type code for Ethernet-encapsulated packets, or a DSAP/SSAP pair for 802.3 or 802.5-encapsulated packets. Ethernet type codes are listed in the appendix "Ethernet Type Codes."
	<i>wild-mask</i>	16-bit hexadecimal number whose ones bits correspond to bits in the <i>type-code</i> argument that should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be at least 0x0101. This is because these two bits are used for purposes other than identifying the SAP codes.)

## bridge acquire

To forward any frames for stations that the system has learned about dynamically, use the **bridge acquire** global configuration command. To disable the behavior, use the **no** form of this command.

**bridge** *bridge-group* **acquire**

**no bridge** *bridge-group* **acquire**

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
---------------------------	---------------------	--

## bridge address

To filter frames with a particular MAC-layer station source or destination address, use the **bridge address** global configuration command. To disable the forwarding ability, use the **no** form of this command.

**bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface*]

**no bridge** *bridge-group* **address** *mac-address*

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number. It must be the same number specified in the <b>bridge protocol</b> command.
	<i>mac-address</i>	48-bit hardware address written as a dotted triple of four-digit hexadecimal numbers such as that displayed by the EXEC <b>show arp</b> command, for example, 0800.cb00.45e9. It is either a station address, the broadcast address, or a multicast destination address.
	<b>forward</b>	Frame sent from or destined to the specified address is forwarded as appropriate.

<b>discard</b>	Frame sent from or destined to the specified address is discarded without further processing.
<i>interface</i>	(Optional) Interface specification, such as Ethernet 0. It is added after the <b>forward</b> or <b>discard</b> keyword to indicate the interface on which that address can be reached.

## bridge bitswap-layer3-addresses

To enable transparent bridging or source-route translational bridging or IP ARPs between canonical and noncanonical media types, use the **bridge bitswap-layer3-addresses** global configuration command. To revert to the default setting, use the **no** form of this command.

**bridge** *bridge-group* **bitswap-layer3-addresses**

**no bridge** *bridge-group* **bitswap-layer3-addresses**

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number.
---------------------------	---------------------	----------------------

## bridge bridge

To enable the bridging of a specified protocol in a specified bridge group, use the **bridge bridge** global configuration command. To disable the bridging of a specified protocol in a specified bridge group, use the **no** form of this command.

**bridge** *bridge-group* **bridge protocol**

**no bridge** *bridge-group* **bridge protocol**

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number. It must be the same number specified in the <b>bridge protocol</b> command.
	<i>protocol</i>	Any of the supported routing protocols. The default is to bridge all of these protocols.

## bridge circuit-group pause

To configure the interval during which transmission is suspended in a circuit group after circuit group changes take place, use the **bridge circuit-group pause** global configuration command.

**bridge** *bridge-group* **circuit-group** *circuit-group* **pause** *milliseconds*

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
	<i>circuit-group</i>	Number of the circuit group to which the interface belongs.
	<i>milliseconds</i>	Forward delay interval. It must be a value in the range 0 to 10000 ms.

## bridge circuit-group source-based

To use just the source MAC address for selecting the output interface, use the **bridge circuit-group source-based** global configuration command. To remove the interface from the bridge group, use the **no** form of this command.

**bridge** *bridge-group* **circuit-group** *circuit-group* **source-based**

**no bridge** *bridge-group* **circuit-group** *circuit-group* **source-based**

---

**Syntax Description**

<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
<i>circuit-group</i>	Number of the circuit group to which the interface belongs.

---

## bridge cmf

To enable constrained multicast flooding (CMF) for all configured bridge groups, use the **bridge cmf** global configuration command. To disable constrained multicast flooding, use the **no** form of this command.

**bridge cmf**

**no bridge cmf**

---

**Syntax Description**

This command has no arguments or keywords.

## bridge crb

To enable the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router, use the **bridge crb** global configuration command. To disable the feature, use the **no** form of this command.

**bridge crb**

**no bridge crb**

---

**Syntax Description**

This command has no arguments or keywords.

## bridge domain

To establish a domain by assigning it a decimal value from 1 and 10, use the **bridge domain** global configuration command. To return to a single bridge domain by choosing domain zero (0), use the **no** form of this command.

**bridge** *bridge-group* **domain** *domain-number*

**no bridge** *bridge-group* **domain**

Syntax Description		
<i>bridge-group</i>		Bridge group number specified in the <b>bridge protocol ieee</b> command. The <b>dec</b> keyword is not valid for this command.
<i>domain-number</i>		Domain ID number you choose. The default domain number is zero; this is the domain number required when communicating to IEEE bridges that do not support this domain extension.

## bridge forward-time

To specify the forward delay interval for the Cisco IOS software, use the **bridge forward-time** global configuration command. To return to the default interval, use the **no** form of this command.

**bridge** *bridge-group* **forward-time** *seconds*

**no bridge** *bridge-group* **forward-time** *seconds*

Syntax Description		
<i>bridge-group</i>		Bridge group number specified in the <b>bridge protocol</b> command.
<i>seconds</i>		Forward delay interval. It must be a value in the range 10 to 200 seconds. The default is 30 seconds.

## bridge-group

To assign each network interface to a bridge group, use the **bridge-group** interface configuration command. To remove the interface from the bridge group, use the **no** form of this command.

**bridge-group** *bridge-group*

**no bridge-group** *bridge-group*

Syntax Description		
<i>bridge-group</i>		Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.

## bridge-group aging-time

To set the length of time that a dynamic entry can remain in the bridge table from the time the entry was created or last updated, use the **bridge-group aging-time** global configuration command. To return to the default aging-time interval, use the **no** form of this command.

**bridge-group** *bridge-group* **aging-time** *seconds*

**no bridge-group** *bridge-group* **aging-time**

Syntax Description		
	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>seconds</i>	Aging time, in the range 0 to 1000000 seconds. The default is 300 seconds.

## bridge-group cbus-bridging

To enable autonomous bridging on a ciscoBus2 controller, use the **bridge-group cbus-bridging** interface configuration command. To disable autonomous bridging, use the **no** form of this command.

**bridge-group** *bridge-group* **cbus-bridging**

**no bridge-group** *bridge-group* **cbus-bridging**

Syntax Description		
	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.

## bridge-group circuit-group

To assign each network interface to a bridge group, use the **bridge-group circuit-group** interface configuration command. To remove the interface from the bridge group, use the **no** form of this command.

**bridge-group** *bridge-group* **circuit-group** *circuit-group*

**no bridge-group** *bridge-group* **circuit-group** *circuit-group*

Syntax Description		
	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>circuit-group</i>	Circuit group number. The range is 1 to 9.

## bridge-group input-address-list

To assign an access list to a particular interface, use the **bridge-group input-address-list** interface configuration command. This access list is used to filter packets received on that interface based on their MAC source addresses. To remove an access list from an interface, use the **no** form of this command.

**bridge-group** *bridge-group* **input-address-list** *access-list-number*

**no bridge-group** *bridge-group* **input-address-list** *access-list-number*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>access-list-number</i>	Access list number you assigned with the <b>access-list</b> command. It must be in the range 700 to 799.

## bridge-group input-lat-service-deny

To specify the group codes by which to deny access upon input, use the **bridge-group input-lat-service-deny** interface configuration command. To remove this access condition, use the **no** form of this command.

**bridge-group** *bridge-group* **input-lat-service-deny** *group-list*

**no bridge-group** *bridge-group* **input-lat-service-deny** *group-list*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>group-list</i>	List of LAT service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

## bridge-group input-lat-service-permit

To specify the group codes by which to permit access upon input, use the **bridge-group input-lat-service-permit** interface configuration command. To remove this access condition, use the **no** form of this command.

**bridge-group** *bridge-group* **input-lat-service-permit** *group-list*

**no bridge-group** *bridge-group* **input-lat-service-permit** *group-list*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>group-list</i>	LAT service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

## bridge-group input-lsap-list

To filter IEEE 802.2-encapsulated packets on input, use the **bridge-group input-lsap-list** interface configuration command. To disable this capability, use the **no** form of this command.

**bridge-group** *bridge-group* **input-lsap-list** *access-list-number*

**no bridge-group** *bridge-group* **input-lsap-list** *access-list-number*

Syntax Description		
<i>bridge-group</i>		Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
<i>access-list-number</i>		Access list number you assigned with the standard <b>access-list</b> command. Specify a zero (0) to disable the application of the access list on the bridge group.

## bridge-group input-pattern-list

To associate an extended access list with a particular interface in a particular bridge group, use the **bridge-group input-pattern-list** interface configuration command. To disable this capability, use the **no** form of this command.

**bridge-group** *bridge-group* **input-pattern-list** *access-list-number*

**no bridge-group** *bridge-group* **input-pattern-list** *access-list-number*

Syntax Description		
<i>bridge-group</i>		Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
<i>access-list-number</i>		Access list number you assigned using the extended <b>access-list</b> command. Specify a zero (0) to disable the application of the access list on the interface.

## bridge-group input-type-list

To filter Ethernet- and SNAP-encapsulated packets on input, use the **bridge-group input-type-list** interface configuration command. To disable this capability, use the **no** form of this command.

**bridge-group** *bridge-group* **input-type-list** *access-list-number*

**no bridge-group** *bridge-group* **input-type-list** *access-list-number*

Syntax Description		
<i>bridge-group</i>		Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
<i>access-list-number</i>		Access list number you assigned with the standard <b>access-list</b> command. Specify a zero (0) to disable the application of the access list on the bridge group.

## bridge-group lat-compression

To reduce the amount of bandwidth that LAT traffic consumes on the serial interface by specifying a LAT-specific form of compression, use the **bridge-group lat-compression** interface configuration command. To disable LAT compression on the bridge group, use the **no** form of this command.

**bridge-group** *bridge-group* **lat-compression**

**no bridge-group** *bridge-group* **lat-compression**

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
---------------------------	---------------------	--

## bridge-group output-address-list

To assign an access list to a particular interface for filtering the MAC destination addresses of packets that would ordinarily be forwarded out that interface, use the **bridge-group output-address-list** interface configuration command. To remove an access list from an interface, use the **no** form of this command.

**bridge-group** *bridge-group* **output-address-list** *access-list-number*

**no bridge-group** *bridge-group* **output-address-list** *access-list-number*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>access-list-number</i>	Access list number you assigned with the standard <b>access-list</b> command.

## bridge-group output-lat-service-deny

To specify the group codes by which to deny access upon output, use the **bridge-group output-lat-service-deny** interface configuration command. To cancel the specified group codes, use the **no** form of this command.

**bridge-group** *bridge-group* **output-lat-service-deny** *group-list*

**no bridge-group** *bridge-group* **output-lat-service-deny** *group-list*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>group-list</i>	List of LAT groups. Single numbers and ranges are permitted.

## bridge-group output-lat-service-permit

To specify the group codes by which to permit access upon output, use the **bridge-group output-lat-service-permit** interface configuration command. To cancel specified group codes, use the **no** form of this command.

**bridge-group** *bridge-group* **output-lat-service-permit** *group-list*

**no bridge-group** *bridge-group* **output-lat-service-permit** *group-list*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>group-list</i>	LAT service advertisements.

## bridge-group output-lsap-list

To filter IEEE 802-encapsulated packets on output, use the **bridge-group output-lsap-list** interface configuration command. To disable this capability, use the **no** form of this command.

**bridge-group** *bridge-group* **output-lsap-list** *access-list-number*

**no bridge-group** *bridge-group* **output-lsap-list** *access-list-number*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>access-list-number</i>	Access list number you assigned with the standard <b>access-list</b> command. Specify a zero (0) to disable the application of the access list on the bridge group.

## bridge-group output-pattern-list

To associate an extended access list with a particular interface, use the **bridge-group output-pattern-list** interface configuration command. To disable this capability, use the **no** form of this command.

**bridge-group** *bridge-group* **output-pattern-list** *access-list-number*

**no bridge-group** *bridge-group* **output-pattern-list** *access-list-number*

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
	<i>access-list-number</i>	Extended access list number you assigned using the extended <b>access-list</b> command. Specify a zero (0) to disable the application of the access list on the interface.

## bridge-group output-type-list

To filter Ethernet- and SNAP-encapsulated packets on output, use the **bridge-group output-type-list** interface configuration command. To disable this capability, use the **no** form of this command.

**bridge-group** *bridge-group* **output-type-list** *access-list-number*

**no bridge-group** *bridge-group* **output-type-list** *access-list-number*

Syntax Description		
<i>bridge-group</i>		Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
<i>access-list-number</i>		Access list number you assigned with the standard <b>access-list</b> command. Specify a zero (0) to disable the application of the access list on the bridge group. This access list is applied just before sending out a frame to an interface.

## bridge-group path-cost

To set a different path cost, use the **bridge-group path-cost** interface configuration command. To choose the default path cost for the interface, use the **no** form of this command.

**bridge-group** *bridge-group* **path-cost** *cost*

**no bridge-group** *bridge-group* **path-cost** *cost*

Syntax Description		
<i>bridge-group</i>		Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
<i>cost</i>		Relative cost of using the path. Path cost can range from 1 to 65535, with higher values indicating higher costs. This range applies regardless of whether the IEEE or Digital Spanning Tree Protocol has been specified.

## bridge-group priority

To set an interface priority, use the **bridge-group priority** interface configuration command. The interface priority is used to select the designated port for this bridge-group on the connected media. One designated port on each media is needed to compute the spanning tree.

**bridge-group** *bridge-group* **priority** *number*

Syntax Description		
<i>bridge-group</i>		Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
<i>number</i>		Priority number ranging from 0 to 255 (Digital), or 0 to 64000 (IEEE).

## bridge-group spanning-disabled

To disable the spanning tree on a given interface, use the **bridge-group spanning-disabled** interface configuration command.

**bridge-group** *bridge-group* **spanning-disabled**

**no bridge-group** *bridge-group* **spanning-disabled**

---

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range of 1 to 63.
---------------------------	---------------------	---

---

## bridge-group sse

To enable the Cisco silicon switching engine (SSE) switching function, use the **bridge-group sse** interface configuration command. To disable SSE switching, use the **no** form of this command.

**bridge-group** *bridge-group* **sse**

**no bridge-group** *bridge-group* **sse**

---

<b>Syntax Description</b>	<i>bridge-group</i>	Number of the bridge group to which the interface belongs. It must be a number in the range 1 to 63.
---------------------------	---------------------	--

---

## bridge-group subscriber-loop-control

To enable loop control on virtual circuits associated with a bridge group, use the **bridge-group subscriber-loop-control** interface configuration command. To disable loop control, use the **no** form of this command.

**bridge-group** *bridge-group* **subscriber-loop-control**

**no bridge-group** *bridge-group* **subscriber-loop-control**

---

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number, in the range from 1 to 256, specified in the <b>bridge protocol</b> command.
---------------------------	---------------------	---

---

## bridge-group subscriber-trunk

To specify that an interface is at the upstream point of traffic flow, use the **bridge-group subscriber-trunk** interface configuration command. To remove the specification and reset the interface to a non-trunking port, use the **no** form of this command.

**bridge-group** *bridge-group* **subscriber-trunk**

**no bridge-group** *bridge-group* **subscriber-trunk**

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number, in the range from 1 to 256, specified in the <b>bridge protocol</b> command.
---------------------------	---------------------	---

## bridge hello-time

To specify the interval between hello bridge protocol data units (BPDUs), use the **bridge hello-time** global configuration command. To return the default interval, use the **no** form of this command.

**bridge** *bridge-group* **hello-time** *seconds*

**no bridge** *bridge-group* **hello-time**

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number. It must be the same number specified in the <b>bridge protocol</b> command.
	<i>seconds</i>	Interval between 1 and 10 seconds.

## bridge irb

To enable the Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups, use the **bridge irb** global configuration command. To disable the feature, use the **no** form of this command.

**bridge irb**

**no bridge irb**

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

## bridge lat-service-filtering

To specify LAT group-code filtering, use the **bridge lat-service-filtering** global configuration command. To disable the use of LAT service filtering on the bridge group, use the **no** form of this command.

**bridge** *bridge-group* **lat-service-filtering**

**no bridge** *bridge-group* **lat-service-filtering**

---

### Syntax Description

<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
---------------------	--

## bridge max-age

To change the interval the bridge will wait to hear BPDUs from the root bridge, use the **bridge max-age** global configuration command. If a bridge does not hear BPDUs from the root bridge within this specified interval, it assumes that the network has changed and will recompute the spanning-tree topology. To return to the default interval, use the **no** form of this command.

**bridge** *bridge-group* **max-age** *seconds*

**no bridge** *bridge-group* **max-age**

---

### Syntax Description

<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
<i>seconds</i>	Interval the bridge will wait to hear BPDUs from the root bridge. It must be a value in the range 10 to 200 seconds.

## bridge multicast-source

To configure bridging support to allow the forwarding, but not the learning, of frames received with multicast source addresses, use the **bridge multicast-source** global configuration command. To disable this function on the bridge, use the **no** form of this command.

**bridge** *bridge-group* **multicast-source**

**no bridge** *bridge-group* **multicast-source**

---

### Syntax Description

<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
---------------------	--

## bridge priority

To configure the priority of an individual bridge, or the likelihood that it will be selected as the root bridge, use the **bridge priority** global configuration command.

**bridge** *bridge-group* **priority** *number*

### Syntax Description

<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
<i>number</i>	The lower the number, the more likely the bridge will be chosen as root. When the IEEE Spanning Tree Protocol is enabled, <i>number</i> ranges from 0 to 65535 (default is 32768). When the Digital Spanning Tree Protocol is enabled, <i>number</i> ranges from 0 to 255 (default is 128).

## bridge protocol

To define the type of Spanning Tree Protocol, use the **bridge protocol** global configuration command. To delete the bridge group, use the **no** form of this command with the appropriate keywords and arguments.

**bridge** *bridge-group* **protocol** {**dec** | **ibm** | **ieee** | **vlan-bridge**}

**no bridge** *bridge-group* **protocol** {**dec** | **ibm** | **ieee** | **vlan-bridge**}

### Syntax Description

<i>bridge-group</i>	Number in the range 1 to 63 that you choose to refer to a particular set of bridged interfaces. Frames are bridged only among interfaces in the same group. You will use the group number you assign in subsequent bridge configuration commands.
<b>dec</b>	Digital Spanning Tree Protocol.
<b>ibm</b>	IBM Spanning Tree Protocol.
<b>ieee</b>	IEEE Ethernet Spanning Tree Protocol.
<b>vlan-bridge</b>	VLAN-Bridge Spanning Tree Protocol.

## bridge route

To enable the routing of a specified protocol in a specified bridge group, use the **bridge route** global configuration command. To disable the routing of a specified protocol in a specified bridge group, use the **no** form of this command.

**bridge** *bridge-group* **route** *protocol*

**no bridge** *bridge-group* **route** *protocol*

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number. It must be the same number specified in the <b>bridge protocol</b> command.
	<i>protocol</i>	One of the following protocols: <b>apollo</b> , <b>appletalk</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , <b>ipx</b> , <b>vines</b> , <b>xns</b> .

## bridge subscriber-policy

To bind a bridge group with a subscriber policy, use the **bridge subscriber-policy** global configuration command. To disable the subscriber bridge group feature, use the **no** form of this command.

**bridge** *bridge-group* **subscriber-policy** *policy*

**no bridge** *bridge-group* **subscriber-policy** *policy*

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number, in the range of 1 to 256, specified in the <b>bridge protocol</b> command.
	<i>policy</i>	Subscriber policy number in the range of 1 to 100.

## clear bridge

To remove any learned entries from the forwarding database and to clear the transmit and receive counts for any statically or system-configured entries, use the **clear bridge** privileged EXEC command.

**clear bridge** *bridge-group*

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
---------------------------	---------------------	--

## clear bridge multicast

To clear transparent bridging multicast state information, use the **clear bridge multicast** EXEC command.

**clear bridge** [*bridge-group*] **multicast** [**router-ports** | **groups** | **counts**]  
[*group-address*] [*interface-unit*] [**counts**]

<b>Syntax Description</b>	<i>bridge-group</i>	(Optional) Bridge group number specified in the <b>bridge protocol</b> command.
	<b>router-ports</b>	(Optional) Clear multicast router ports.
	<b>groups</b>	(Optional) Clear multicast groups.
	<b>counts</b>	(Optional) Clear RX and TX counts.
	<i>group-address</i>	(Optional) Multicast IP address associated with a specific multicast group.
	<i>interface-unit</i>	(Optional) Specific interface, such as Ethernet 0.

## clear vlan statistics

To remove virtual LAN statistics from any statically or system-configured entries, use the **clear vlan statistics** privileged EXEC command.

**clear vlan statistics**

---

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

## frame-relay map bridge broadcast

To bridge over a Frame Relay network, use the **frame-relay map bridge broadcast** interface configuration command. To delete the mapping entry, use the **no** form of this command.

**frame-relay map bridge** *dlci* **broadcast**

**no frame-relay map bridge** *dlci* **broadcast**

---

**Syntax Description** *dlci* DLCI number. The valid range is 16 to 1007.

---

## interface bvi

To create the bridge-group virtual interface (BVI) that represents the specified bridge group to the routed world and links the corresponding bridge group to the other routed interfaces, use the **interface bvi** interface configuration command. To delete the BVI, use the **no** form of this command.

**interface bvi** *bridge-group*

**no interface bvi** *bridge-group*

---

**Syntax Description** *bridge-group* Bridge group number. It must be the same number specified in the **bridge protocol** command.

---

## show bridge

To display classes of entries in the bridge forwarding database, use the **show bridge** privileged EXEC command.

**show bridge** [*bridge-group*] [*interface*] [*address* [*mask*]] [**verbose**]

---

**Syntax Description** *bridge-group* (Optional) Number that specifies a particular spanning tree.

---

*interface* (Optional) Specific interface, such as Ethernet 0.

---

<i>address</i>	(Optional) 48-bit canonical (Ethernet ordered) MAC address. This may be entered with an optional mask of bits to be ignored in the address, which is specified with the <i>mask</i> argument.
<i>mask</i>	(Optional) Bits to be ignored in the address. You must specify the <i>address</i> argument if you want to specify a mask.
<b>verbose</b>	(Optional) Displays additional detail, including any Frame Relay DLCI associated with a station address.

## show bridge circuit-group

To display the interfaces configured in each circuit group and show whether they are currently participating in load distribution, use the **show bridge circuit-group** EXEC command.

```
show bridge [bridge-group] circuit-group [circuit-group] [src-mac-address] [dst-mac-address]
```

### Syntax Description

<i>bridge-group</i>	(Optional) Number that specifies a particular bridge group.
<i>circuit-group</i>	(Optional) Number that specifies a particular circuit group.
<i>src-mac-address</i>	(Optional) 48-bit canonical (Ethernet ordered) source MAC address.
<i>dst-mac-address</i>	(Optional) 48-bit canonical (Ethernet ordered) destination MAC address.

## show bridge group

To display the status of each bridge group, use the **show bridge group** privileged EXEC command.

```
show bridge group [verbose]
```

### Syntax Description

<b>verbose</b>	(Optional) Displays detailed information.
----------------	---

## show bridge multicast

To display transparent bridging multicast state information, use the **show bridge multicast** EXEC command.

```
show bridge [bridge-group] multicast [router-ports | groups] [group-address]
```

### Syntax Description

<i>bridge-group</i>	(Optional) Bridge group number specified in the <b>bridge protocol</b> command.
<b>router-ports</b>	(Optional) Display information for multicast router ports.
<b>groups</b>	(Optional) Display information for multicast groups.
<i>group-address</i>	(Optional) Multicast IP address associated with a specific multicast group.

## show bridge vlan

To display virtual LAN subinterfaces, use the **show bridge vlan** privileged EXEC command.

```
show bridge vlan
```

---

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

## show interfaces crb

To display the configuration for each interface that has been configured for routing or bridging, use the **show interfaces crb** privileged EXEC command.

```
show interfaces crb
```

---

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

## show interfaces irb

To display the configuration for each interface that has been configured for integrated routing or bridging, use the **show interfaces irb** privileged EXEC command.

```
show interfaces { ethernet | fastethernet } [interface | slot/port] irb
```

---

**Syntax Description**

<b>ethernet</b>	Specify Ethernet interface.
<b>fastethernet</b>	Specify Fast Ethernet interface.
<i>interface</i>	(Optional) Specific interface, such as Ethernet 0.
<i>slot/port</i>	(Optional) Specific slot/port, such as Fast Ethernet 3/0.

## show spanning-tree

To display information regarding which Spanning Tree Protocol is running, use the **show spanning-tree** configuration command.

```
show spanning-tree bridge-group
```

---

**Syntax Description**

<i>bridge-group</i>	Bridge group number, in the range of 1 to 256, specified in the <b>bridge protocol</b> command.
---------------------	---

## show subscriber-policy

To display the details of a subscriber policy, use the **show subscriber-policy** EXEC command.

```
show subscriber-policy range
```

Syntax Description	
<i>range</i>	Range of subscriber policy numbers (range 1 to 100).

## 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.

## subscriber-policy

To define or modify the forward and filter decisions of the subscriber policy, use the **subscriber-policy** global configuration command. To restore the default forward and filter values, use the **no** or **default** form of this command.

```
subscriber-policy policy [[no | default] packet [permit | deny]]
```

Syntax Description	
<i>policy</i>	Subscriber policy number in the range 1 to 100.
<b>no</b>	(Optional) Turn off the permit for the packet (this is an equivalent of the <b>deny</b> keyword).
<b>default</b>	(Optional) Deny forwarding of the packet (this is an equivalent of the <b>deny</b> keyword).
<i>packet</i>	(Optional) One of the following packets: <ul style="list-style-type: none"> <li>• <i>arp</i></li> <li>• <i>broadcast</i></li> <li>• <i>cdp</i></li> <li>• <i>multicast</i></li> <li>• <i>st</i></li> <li>• <i>unknown unicast</i></li> </ul>
<b>permit</b>	(Optional) Permit forwarding of the packet.
<b>deny</b>	(Optional) Deny forwarding of the packet.

## x25 map bridge

To configure the an Internet-to-X.121 address mapping for bridging over X.25, use the **x25 map bridge** interface configuration command. To disable the Internet-to-X.121 mapping, use the **no** form of this command.

**x25 map bridge** *x.121-address* **broadcast** [*options-keywords*]

**no x25 map bridge** *x.121-address* **broadcast** [*options-keywords*]

### Syntax Description

<i>x.121-address</i>	The X.121 address.
<b>broadcast</b>	Required keyword for bridging over X.25.
<i>options-keywords</i>	(Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 3.

The X.25 bridging implementation supports the map options listed in Table 3.

**Table 3** X.25 Map Options

Option	Description
<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 to its impact on overall performance.
<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 uses 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>idle</b> <i>minutes</i>	Specifies an idle timeout for calls other than the interface default; 0 minutes disables the idle timeout.
<b>reverse</b>	Specifies reverse charging for outgoing calls.

Table 3 X.25 Map Options (continued)

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 number (from 1 to 99) for the mapping in an outgoing call.
<b>nvc count</b>	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 in-size out-size</b>	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>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.
<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>nuid username password</b>	Specifies that a network user ID (NUID) facility be sent in the outgoing call with the specified Terminal Access Controller Access Control System (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.
<b>nudata string</b>	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.
<b>rpoa name</b>	Specifies the name defined by the <b>x25 roa</b> command for a list of transit Recognized Operating Agencies (ROAs) to use in outgoing Call Request packets.
<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.





## Source-Route Bridging Commands

---

This chapter describes the function and syntax of the source-route bridging (SRB) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### access-expression

To define an access expression, use the **access-expression** interface configuration command. To remove the access expression from the given interface, use the **no** form of this command.

```
access-expression {in | out} expression
```

```
no access-expression {in | out} expression
```

---

#### Syntax Description

<b>in   out</b>	Either <b>in</b> or <b>out</b> is specified to indicate whether the access expression is applied to packets entering or leaving this interface. You can specify both an input and an output access expression for an interface, but only one of each.
<i>expression</i>	Boolean access list expression.

---

### access-list

To configure the access list mechanism for filtering frames by protocol type or vendor code, use the **access-list** global configuration command. To remove the single specified entry from the access list, use the **no** form of this command.

```
access-list access-list-number {permit | deny} {type-code wild-mask | address mask}
```

```
no access-list access-list-number {permit | deny} {type-code wild-mask | address mask}
```

---

#### Syntax Description

<i>access-list-number</i>	Integer that identifies the access list. If the <i>type-code wild-mask</i> arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the <i>address</i> and <i>mask</i> arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code.
<b>permit</b>	Permits the frame.

---

<b>deny</b>	Denies the frame.
<i>type-code</i>	16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a SNAP type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.)
<i>wild-mask</i>	16-bit hexadecimal number whose ones bits correspond to bits in the <i>type-code</i> argument. The <i>wild-mask</i> indicates which bits in the <i>type-code</i> argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.)
<i>address</i>	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. This field is used for filtering by vendor code.
<i>mask</i>	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. The ones bits in <i>mask</i> are the bits to be ignored in <i>address</i> . This field is used for filtering by vendor code.

For source address filtering, the mask always should have the high-order bit set. This is because the IEEE 802 standard uses this bit to indicate whether a RIF is present, not as part of the source address.

## bridge protocol ibm

To create a bridge group that runs the automatic spanning-tree function, use the **bridge protocol ibm** global configuration command. To cancel the previous assignment, use the **no** form of this command.

**bridge** *bridge-group* **protocol ibm**

**no bridge** *bridge-group* **protocol ibm**

<b>Syntax Description</b>	<i>bridge-group</i>	Number in the range 1 to 9 that you choose to refer to a particular set of bridged interfaces.
---------------------------	---------------------	--

## clear netbios-cache

To clear the entries of all dynamically learned NetBIOS names, use the **clear netbios-cache** privileged EXEC command. This command will not remove statically defined name cache entries.

**clear netbios-cache**

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

## clear rif-cache

To clear the entire RIF cache, use the **clear rif-cache** privileged EXEC command.

```
clear rif-cache
```

---

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

## clear source-bridge

To clear the source-bridge statistical counters, use the **clear source-bridge** privileged EXEC command.

```
clear source-bridge
```

---

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

## clear sse

To reinitialize the Silicon Switch Processor (SSP) on the Cisco 7000 series routers with RSP7000, use the **clear sse** privileged EXEC command.

```
clear sse
```

---

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

## ethernet-transit-oui

To choose the Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks, use the **ethernet-transit-oui** interface configuration command. Various versions of this OUI code are used by Ethernet/Token Ring translational bridges. To return the default OUI code, use the **no** form of this command.

```
ethernet-transit-oui [90-compatible | standard | cisco]
```

```
no ethernet-transit-oui
```

---

<b>Syntax Description</b>	<b>90-compatible</b>	(Optional) Default OUI form.
	<b>standard</b>	(Optional) Standard OUI form.
	<b>cisco</b>	(Optional) Cisco's OUI form.

---

## Inm alternate

To specify the threshold reporting link number, use the **Inm alternate** interface configuration command. In order for a LAN Reporting Manager (LRM) to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number. To restore the default of 0, use the **no** form of this command.

**Inm alternate** *number*

**no Inm alternate**

---

<b>Syntax Description</b>	<i>number</i>	Threshold reporting link number. It must be in the range 0 to 3.
---------------------------	---------------	--

---

## Inm crs

To monitor the current logical configuration of a Token Ring, use the **Inm crs** interface configuration command. To disable this function, use the **no** form of this command.

**Inm crs**

**no Inm crs**

---

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

## Inm disabled

To disable LNM functionality, use the **Inm disabled** global configuration command. To restore LNM functionality, use the **no** form of this command.

**Inm disabled**

**no Inm disabled**

---

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

## lnm express-buffer

To enable the LNM RPS express buffer function, use the **lnm express-buffer** interface configuration command. To disable this function, use the **no** form of this command.

**lnm express-buffer**

**no lnm express-buffer**

---

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

## lnm loss-threshold

To set the threshold at which the Cisco IOS software sends a message informing all attached LNMs that it is dropping frames, use the **lnm loss-threshold** interface configuration command. To return to the default value, use the **no** form of this command.

**lnm loss-threshold** *number*

**no lnm loss-threshold**

---

**Syntax Description**

<i>number</i>	Single number expressing the percentage loss rate in hundredths of a percent. The valid range is 0 to 9999.
---------------	---

---

## lnm password

To set the password for the reporting link, use the **lnm password** interface configuration command. To return the password to its default value of 00000000, use the **no** form of this command.

**lnm password** *number string*

**no lnm password** *number*

---

**Syntax Description**

<i>number</i>	Number of the reporting link to which to apply the password. This value should be in the range 0 to 3.
<i>string</i>	Password you enter at the keyboard. In order to maintain compatibility with LNM, the parameter <i>string</i> should be a six- to eight-character string.

---

## Inm pathtrace-disabled

To disable pathtrace reporting to LNM stations, use the **inm pathtrace-disabled** global configuration command. To restore pathtrace reporting functionality, use the **no** form of this command.

**inm pathtrace-disabled** [**all** | **origin**]

**no inm pathtrace-disabled**

---

### Syntax Description

<b>all</b>	(Optional) Disable pathtrace reporting to the LNM and originating stations.
<b>origin</b>	(Optional) Disable pathtrace reporting to originating stations only.

---

## Inm rem

To monitor errors reported by any station on the ring, use the **inm rem** interface configuration command. To disable this function, use the **no** form of this command.

**inm rem**

**no inm rem**

---

### Syntax Description

This command has no arguments or keywords.

## Inm rps

To ensure that all stations on a ring are using a consistent set of reporting parameters, use the **inm rps** interface configuration command. To disable this function, use the **no** form of this command.

**inm rps**

**no inm rps**

---

### Syntax Description

This command has no arguments or keywords.

## Inm snmp-only

To prevent any LNM stations from modifying parameters in the Cisco IOS software, use the **inm snmp-only** global configuration command. To allow modifications, use the **no** form of this command.

**inm snmp-only**

**no inm snmp-only**

---

### Syntax Description

This command has no arguments or keywords.

## Inm softerr

To set the time interval in which the Cisco IOS software will accumulate error messages before sending them, use the **Inm softerr** interface configuration command. To return to the default value, use the **no** form of this command.

**Inm softerr** *milliseconds*

**no Inm softerr**

<b>Syntax Description</b>	<i>milliseconds</i>	Time interval in tens of milliseconds between error messages. The valid range is 0 to 65535.
---------------------------	---------------------	--

## mac-address

To set the MAC layer address of the Cisco Token Ring, use the **mac-address** interface configuration command. To return to the default value, use the **no** form of this command.

**mac-address** *ieee-address*

**no mac-address** *ieee-address*

<b>Syntax Description</b>	<i>ieee-address</i>	48-bit IEEE MAC address written as a dotted triple of four-digit hexadecimal numbers.
---------------------------	---------------------	---

## multiring

To enable collection and use of RIF information, use the **multiring** interface configuration command. To disable the use of RIF information for the protocol specified, use the **no** form of this command.

**multiring** {*protocol-keyword* [**all-routes** | **spanning**] | **all** | **other**}

**no multiring** {*protocol-keyword* [**all-routes** | **spanning**] | **all** | **other**}

<b>Syntax Description</b>	<i>protocol-keyword</i>	Specifies a protocol.
	<b>all-routes</b>	(Optional) Uses all-routes explorers.
	<b>spanning</b>	(Optional) Uses spanning-tree explorers.
	<b>all</b>	Enables the multiring for <i>all</i> frames.
	<b>other</b>	Enables the multiring for <i>any</i> routed frame not included in the previous list of supported protocols.

## netbios access-list bytes

To define the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets, use the **netbios access-list bytes** global configuration command. To remove an entire list or the entry specified with the *pattern* argument, use the **no** form of this command.

```
netbios access-list bytes name {permit | deny} offset pattern
```

```
no netbios access-list bytes name {permit | deny} offset pattern
```

### Syntax Description

<i>name</i>	Name of the access list being defined.
<b>permit</b>	Permits the condition.
<b>deny</b>	Denies the condition.
<i>offset</i>	Decimal number indicating the number of bytes into the packet where the byte comparison should begin. An offset of zero points to the very beginning of the NetBIOS header. Therefore, the NetBIOS delimiter string (0xFFEF), for example, begins at offset 2.
<i>pattern</i>	Hexadecimal string of digits representing a byte pattern.

## netbios access-list host

To assign the name of the access list to a station or set of stations on the network, use the **netbios access-list host** global configuration command. The NetBIOS station access list contains the station name to match, along with a permit or deny condition. To remove either an entire list or just a single entry from a list, depending upon the argument given for *pattern*, use the **no** form of this command.

```
netbios access-list host name {permit | deny} pattern
```

```
no netbios access-list host name {permit | deny} pattern
```

### Syntax Description

<i>name</i>	Name of the access list being defined.
<b>permit</b>	Permits the condition.
<b>deny</b>	Denies the condition.
<i>pattern</i>	A set of characters. The characters can be the name of the station, or a combination of characters and pattern-matching symbols that establish a pattern for a set of NetBIOS station names. This combination can be especially useful when stations have names with the same characters, such as a prefix. Table 4 explains the pattern-matching symbols that can be used.

**Table 4** Station Name Pattern-Matching Characters

Character	Description
*	Used at the end of a string to match any character or string of characters.
?	Matches any single character. If this wildcard is used as the first letter of the name, you must precede it with a CNTL-V key sequence. Otherwise it will be interpreted by the router as a request for help.

## netbios enable-name-cache

To enable NetBIOS name caching, use the **netbios enable-name-cache** interface configuration command. To disable the name-cache behavior, use the **no** form of this command.

```
netbios enable-name-cache
```

```
no netbios enable-name-cache
```

---

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

## netbios input-access-filter bytes

To define a byte access list filter on incoming messages, use the **netbios input-access-filter bytes** interface configuration command. The actual access filter byte offsets and patterns used are defined in one or more **netbios-access-list bytes** commands. To remove the entire access list, use the **no** form of this command with the appropriate name.

```
netbios input-access-filter bytes name
```

```
no netbios input-access-filter bytes name
```

---

**Syntax Description** *name* Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list bytes** global configuration commands.

---

## netbios input-access-filter host

To define a station access list filter on incoming messages, use the **netbios input-access-filter host** interface configuration command. To remove the entire access list, use the **no** form of this command with the appropriate argument.

```
netbios input-access-filter host name
```

```
no netbios input-access-filter host name
```

---

**Syntax Description** *name* Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list host** global configuration commands.

---

## netbios name-cache

To define a static NetBIOS name cache entry, tying the server with the name *netbios-name* to the *mac-address*, and specifying that the server is accessible either locally through the *interface-name* specified, or remotely, through the **ring-group** *group-number* specified, use the **netbios name-cache** global configuration command. To remove the entry, use the **no** form of this command.

```
netbios name-cache mac-address netbios-name { interface-name | ring-group group-number }
```

```
no netbios name-cache mac-address netbios-name
```

Syntax Description		
	<i>mac-address</i>	The MAC address.
	<i>netbios-name</i>	Server name linked to the MAC address.
	<i>interface-name</i>	Name of the interface by which the server is accessible locally.
	<b>ring-group</b>	Specifies that the link is accessible remotely.
	<i>group-number</i>	Number of the ring group by which the server is accessible remotely. This ring group number must match the number you have specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.

## netbios name-cache name-len

To specify how many characters of the NetBIOS type name the name cache will validate, use the **netbios name-cache name-len** global configuration command.

```
netbios name-cache name-len length
```

```
no netbios name-cache name-len length
```

Syntax Description		
	<i>length</i>	Length of the NetBIOS type name. The range is 8 to 16 characters.

## netbios name-cache proxy-datagram

To enable the Cisco IOS software to act as a proxy and send NetBIOS datagram type frames, use the **netbios name-cache proxy-datagram** global configuration command. To return to the default value, use the **no** form of this command.

```
netbios name-cache proxy-datagram seconds
```

```
no netbios name-cache proxy-datagram seconds
```

Syntax Description		
	<i>seconds</i>	Time interval, in seconds, that the software forwards a route broadcast datagram type packet. The valid range is any number greater than 0.

## netbios name-cache query-timeout

To specify the “dead” time, in seconds, that starts when a host sends any ADD\_NAME\_QUERY, ADD\_GROUP\_NAME, or STATUS\_QUERY frame, use the **netbios name-cache query-timeout** global configuration command. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD\_NAME\_QUERY, ADD\_GROUP\_NAME, or STATUS\_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process. To restore the default of 6 seconds, use the **no** form of this command.

**netbios name-cache query-timeout** *seconds*

**no netbios name-cache query-timeout**

---

### Syntax Description

*seconds*

Dead time period in seconds. Default is 6 seconds.

---

## netbios name-cache recognized-timeout

To specify the “dead” time, in seconds, that starts when a host sends any FIND\_NAME or NAME\_RECOGNIZED frame, use the **netbios name-cache recognized-timeout** global configuration command. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND\_NAME or NAME\_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process. To restore the default of 6 seconds, use the **no** form of this command.

**netbios name-cache recognized-timeout** *seconds*

**no netbios name-cache recognized-timeout**

---

### Syntax Description

*seconds*

Dead time period in seconds. Default is 6 seconds.

---

## netbios name-cache timeout

To enable NetBIOS name caching and to set the time that entries can remain in the NetBIOS name cache, use the **netbios name-cache timeout** global configuration command. To restore the default of 15 minutes, use the **no** form of this command.

**netbios name-cache timeout** *minutes*

**no netbios name-cache timeout** *minutes*

---

### Syntax Description

*minutes*

Time, in minutes, that entries can remain in the NetBIOS name cache. Once the time expires, the entry will be deleted from the cache. Default is 15 minutes.

---

## netbios output-access-filter bytes

To define a byte access list filter on outgoing messages, use the **netbios output-access-filter bytes** interface configuration command. To remove the entire access list, use the **no** form of this command.

**netbios output-access-filter bytes** *name*

**no netbios output-access-filter bytes** *name*

<b>Syntax Description</b>	<i>name</i>	Name of a NetBIOS access filter previously defined with one or more of the <b>netbios access-list bytes</b> global configuration commands.
---------------------------	-------------	--

## netbios output-access-filter host

To define a station access list filter on outgoing messages, use the **netbios output-access-filter host** interface configuration command. To remove the entire access list, use the **no** form of this command.

**netbios output-access-filter host** *name*

**no netbios output-access-filter host** *name*

<b>Syntax Description</b>	<i>name</i>	Name of a NetBIOS access filter previously defined with one or more of the <b>netbios access-list host</b> global configuration commands.
---------------------------	-------------	---

## rif

To enter static source-route information into the Routing Information Field (RIF) cache, use the **rif** global configuration command. If a Token Ring host does not support the use of IEEE 802.2 TEST or XID datagrams as explorer packets, you may need to add static information to the RIF cache of the router. To remove an entry from the cache, use the **no** form of this command.

**rif** *mac-address rif-string* { *interface-name* | **ring-group** *ring* }

**no rif** *mac-address rif-string* { *interface-name* | **ring-group** *ring* }

<b>Syntax Description</b>	<i>mac-address</i>	12-digit hexadecimal string written as a dotted triple of four-digit hexadecimal numbers; for example, 0010.0a00.20a6.
	<i>rif-string</i>	Series of 4-digit hexadecimal numbers separated by a period (.). This RIF string is inserted into the packets sent to the specified MAC address.
	<i>interface-name</i>	Interface name (for example, tokenring 0) that indicates the origin of the RIF.
	<b>ring-group</b>	Specifies the origin of the RIF is a ring group.
	<i>ring</i>	Ring group number that indicates the origin of the RIF. This ring group number must match the number you have specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.

## rif timeout

To determine the number of minutes an inactive RIF entry is kept, use the **rif timeout** global configuration command. RIF information is maintained in a cache whose entries are aged. To restore the default, use the **no** form of this command.

**rif timeout** *minutes*

**no rif timeout**

---

<b>Syntax Description</b>	<i>minutes</i>	Number of minutes an inactive RIF entry is kept. The value must be greater than 0. Default is 15 minutes.
---------------------------	----------------	---

---

## rif validate-age

To define the validation time when the Cisco IOS software is acting as a proxy for NetBIOS NAME\_QUERY packet or for explorer frames, use the **rif validate-age** global configuration command.

**rif validate-age** *seconds*

**no rif validate-age** *seconds*

---

<b>Syntax Description</b>	<i>seconds</i>	Interval, in seconds, at which a proxy is sent. The valid range is any number greater than 0. Default is 2 seconds.
---------------------------	----------------	---

---

## rif validate-enable

To enable RIF validation for entries learned on an interface (Token Ring or FDDI), use the **rif validate-enable** global configuration command. To disable the specification, use the **no** form of this command.

**rif validate-enable**

**no rif validate-enable**

---

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

## rif validate-enable-age

To enable RIF validation for stations on a source-route bridge network that do not respond to an IEEE TEST command, use the **rif validate-enable-age** global configuration command. To disable the specification, use the **no** form of this command.

**rif validate-enable-age**

**no rif validate-enable-age**

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

## rif validate-enable-route-cache

To enable synchronization of the RIF cache with the protocol route cache, use the **rif validate-enable-route-cache** global configuration command. To disable the specification, use the **no** form of this command.

**rif validate-enable-route-cache**

**no rif validate-enable-route-cache**

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

## show access-expression

To display the defined input and output access list expressions, use the **show access-expression** privileged EXEC command.

**show access-expression [begin | include | exclude]**

<b>Syntax Description</b>	<b>begin</b>	(Optional) Begin with the access list expression that matches.
	<b>include</b>	(Optional) Include access list expressions that match.
	<b>exclude</b>	(Optional) Exclude access list expressions that match.

## show controllers token (IBM)

To display information about memory management, error counters, and the board itself, use the **show controllers token** privileged EXEC command.

```
show controllers token
```

---

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

## show interfaces tokenring (IBM)

To display information about the Token Ring interface and the state of source-route bridging (SRB), use the **show interfaces tokenring** privileged EXEC command.

```
show interfaces tokenring [number]
```

---

**Syntax Description** *number* (Optional) Interface number. If you do not provide a value, the command will display statistics for all Token Ring interfaces.

---

## show lnm bridge

To display all currently configured bridges and all parameters that are related to the bridge as a whole, not to one of its interfaces, use the **show lnm bridge** privileged EXEC command.

```
show lnm bridge
```

---

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

## show lnm config

To display the logical configuration of all bridges configured in a router, use the **show lnm config** privileged EXEC command. This information is needed to configure an LNM Management Station to communicate with a router. This is especially important when the router is configured as a multiport bridge, thus employing the concept of a virtual ring.

```
show lnm config
```

---

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

## show lnm interface

To display all LNM-related information about a specific interface or all interfaces, use the **show lnm interface** privileged EXEC command.

```
show lnm interface [type number]
```

---

### Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

---

## show lnm ring

To display all LNM information about a specific Token Ring or all Token Rings, use the **show lnm ring** privileged EXEC command. If a specific interface is requested, it also displays a list of all currently active stations on that interface.

```
show lnm ring [ring-number]
```

---

### Syntax Description

<i>ring-number</i>	(Optional) Number of a specific Token Ring. It can be a value in the range 1 to 4095.
--------------------	---

---

## show lnm station

To display LNM-related information about a specific station or all known stations on all rings, use the **show lnm station** privileged EXEC command. If a specific station is requested, it also displays a detailed list of that station's current MAC-level parameters.

```
show lnm station [address]
```

---

### Syntax Description

<i>address</i>	(Optional) Address of a specific LNM station.
----------------	---

---

## show netbios-cache

To display a list of NetBIOS cache entries, use the **show netbios-cache** privileged EXEC command.

```
show netbios cache
```

---

### Syntax Description

This command has no arguments or keywords.

## show rif

To display the current contents of the RIF cache, use the **show rif** privileged EXEC command.

```
show rif
```

---

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

## show source-bridge

To display the current source bridge configuration and miscellaneous statistics, use the **show source-bridge** privileged EXEC command.

```
show source-bridge [interface]
```

---

<b>Syntax Description</b>	<b>interface</b>	(Optional) Displays the current source bridge configuration over all interfaces and a summary of all packets sent and received over each interface, not just the number of packets forwarded through the bridge.
---------------------------	------------------	--

---

## show span

To display the spanning-tree topology known to the router, use the **show span** EXEC command.

```
show span
```

---

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

## source-bridge

To configure an interface for source-route bridging (SRB), use the **source-bridge** interface configuration command. To disable source-route bridging on an interface, use the **no** form of this command.

```
source-bridge source-ring-number bridge-number target-ring-number [conserve-ring]
```

```
no source-bridge source-ring-number bridge-number target-ring-number [conserve-ring]
```

<b>Syntax Description</b>	<i>source-ring-number</i>	Ring number for the interface's Token Ring or FDDI ring. It must be a decimal number in the range 1 to 4095 that uniquely identifies a network segment or ring within the bridged Token Ring or FDDI network
	<i>bridge-number</i>	Number that uniquely identifies the bridge connecting the source and target rings. It must be a decimal number in the range 1 to 15.
	<i>target-ring-number</i>	Ring number of the destination ring on this router. It must be unique within the bridged Token Ring or FDDI network. The target ring can also be a ring group. Must be a decimal number.
	<b>conserve-ring</b>	(Optional) Keyword to enable SRB over Frame Relay. When this option is configured, the SRB software does not add the ring number associated with the Frame Relay PVC (the partner's virtual ring) to outbound explorer frames. This option is permitted for Frame Relay subinterfaces only.

## source-bridge connection-timeout

To establish the interval of time between first attempt to open a connection until a timeout is declared, use the **source-bridge connection-timeout** global configuration command. To disable this feature, use the **no** form of this command.

**source-bridge connection-timeout** *seconds*

**no source-bridge connection-timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Interval of time, in seconds, before a connection attempt to a remote peer is aborted.
---------------------------	----------------	--

## source-bridge enable-80d5

To change the router's Token Ring to Ethernet translation behavior, use the **source-bridge enable-80d5** global configuration command. To disable this function, use the **no** form of this command.

**source-bridge enable-80d5**

**no source-bridge enable-80d5**

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

## source-bridge explorer-dup-ARE-filter

To prevent excessive forwarding of explorers in networks with redundant topologies, use the **source-bridge explorer-dup-ARE-filter** global configuration command. To disable this feature, use the **no** form of this command.

```
source-bridge explorer-dup-ARE-filter
```

```
no source-bridge explorer-dup-ARE-filter
```

---

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

## source-bridge explorer-fastswitch

To enable explorer fast switching, use the **source-bridge explorer-fastswitch** global configuration command. To disable explorer fast switching, use the **no** form of this command.

```
source-bridge explorer-fastswitch
```

```
no source-bridge explorer-fastswitch
```

---

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

## source-bridge explorer-maxrate

To set the maximum byte rate of explorers per ring, use the **source-bridge explorer-maxrate** global configuration command. To reset the default rate, use the **no** form of this command.

```
source-bridge explorer-maxrate maxrate
```

```
no source-bridge explorer-maxrate maxrate
```

---

**Syntax Description**

<i>maxrate</i>	Number in the range 100 to 1000000000 (in bytes per second). The default maximum byte rate is 38400 bytes per second.
----------------	---

---

## source-bridge explorerq-depth

To set the maximum explorer queue depth, use the **source-bridge explorerq-depth** global configuration command. To reset the default value, use the **no** form of this command.

**source-bridge explorerq-depth** *depth*

**no source-bridge explorerq-depth** *depth*

<b>Syntax Description</b>	<i>depth</i>	The maximum number of incoming packets. The valid range is 1 to 500.
---------------------------	--------------	--

## source-bridge input-address-list

To apply an access list to an interface configured for source-route bridging, use the **source-bridge input-address-list** interface configuration command. This command filters source-routed packets received from the router interface based upon the source mac address. To remove the application of the access list, use the **no** form of this command.

**source-bridge input-address-list** *access-list-number*

**no source-bridge input-address-list** *access-list-number*

<b>Syntax Description</b>	<i>access-list-number</i>	Number of the access list. The value must be in the range 700 to 799.
---------------------------	---------------------------	---

## source-bridge input-lsap-list

To filter, on input, FDDI and IEEE 802-encapsulated packets that include the destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats, use the **source-bridge input-lsap-list** interface configuration command. The access list specifying the type codes to be filtered is given by this variation of the **source-bridge** interface configuration command. To restore the default value, use the **no** form of this command.

**source-bridge input-lsap-list** *access-list-number*

**no source-bridge input-lsap-list** *access-list-number*

<b>Syntax Description</b>	<i>access-list-number</i>	Number of the access list. This access list is applied to all IEEE 802 or FDDI frames received on that interface prior to the source-routing process. Specify zero (0) to disable the filter. The value must be in the range 200 to 299.
---------------------------	---------------------------	--

## source-bridge input-type-list

To filter SNAP-encapsulated packets on input, use the **source-bridge input-type-list** interface configuration command.

**source-bridge input-type-list** *access-list-number*

**no source-bridge input-type-list** *access-list-number*

<b>Syntax Description</b>	<i>access-list-number</i>	Number of the access list. This access list is applied to all SNAP frames received on that interface prior to the source-routing process. Specify zero (0) to disable the application of the access list on the bridge group. The value must be in the range 200 to 299.
---------------------------	---------------------------	--

## source-bridge max-hops

To control the forwarding or blocking of all-route explorer frames received on an interface, use the **source-bridge max-hops** interface configuration command. To reset the count to the maximum value, use the **no** form of this command.

**source-bridge max-hops** *count*

**no source-bridge max-hops**

<b>Syntax Description</b>	<i>count</i>	Determines the number of bridges an explorer packet can traverse. Typically, the maximum number of bridges for interoperability with IBM equipment is 7.
---------------------------	--------------	--

## source-bridge max-in-hops

To control the forwarding or blocking of spanning-tree explorer frames received on an interface, use the **source-bridge max-in-hops** interface configuration command. To reset the count to the maximum value, use the **no** form of this command.

**source-bridge max-in-hops** *count*

**no source-bridge max-in-hops**

<b>Syntax Description</b>	<i>count</i>	Determines the number of bridges an explorer packet can traverse. Typically, the maximum number of bridges for interoperability with IBM equipment is 7.
---------------------------	--------------	--

## source-bridge max-out-hops

To control the forwarding or blocking of spanning-tree explorer frames sent from this interface, use the **source-bridge max-out-hops** interface configuration command. To reset the count to the maximum value, use the **no** form of this command.

**source-bridge max-out-hops** *count*

**no source-bridge max-out-hops**

---

### Syntax Description

*count*

Determines the number of bridges an explorer packet can traverse. Typically, the maximum number of bridges for interoperability with IBM equipment is 7.

---

## source-bridge output-address-list

To apply an access list to an interface configured for source-route bridging, use the **source-bridge output-address-list** interface configuration command. This command filters source-routed packets sent to the router interface based upon the destination mac address. To remove the application of the access list, use the **no** form of this command.

**source-bridge output-address-list** *access-list-number*

**no source-bridge output-address-list** *access-list-number*

---

### Syntax Description

*access-list-number*

Number of the access list. The value must be in the range 700 to 799.

---

## source-bridge output-lsap-list

To filter, on output, FDDI and IEEE 802-encapsulated packets that have destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats, use the **source-bridge output-lsap-list** interface configuration command.

**source-bridge output-lsap-list** *access-list-number*

**no source-bridge output-lsap-list** *access-list-number*

---

### Syntax Description

*access-list-number*

Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the filter. The value must be in the range 200 to 299.

---

## source-bridge output-type-list

To filter SNAP-encapsulated frames by type code on output, use the **source-bridge output-type-list** interface configuration command. To restore the default value, use the **no** form of this command.

**source-bridge output-type-list** *access-list-numbers*

**no source-bridge output-type-list** *access-list-numbers*

---

<b>Syntax Description</b>	<i>access-list-number</i>	Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the application of the access list on the bridge group. The value must be in the range 200 to 299.
---------------------------	---------------------------	--

---

## source-bridge proxy-explorer

To configure the interface to respond to any explorer packets from a source node that meet the conditions described below, use the **source-bridge proxy-explorer** interface configuration command. To cancel responding to explorer packets with proxy explorers, use the **no** form of this command.

**source-bridge proxy-explorer**

**no source-bridge proxy-explorer**

---

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

## source-bridge proxy-netbios-only

To enable proxy explorers for the NetBIOS name-caching function, use the **source-bridge proxy-netbios-only** global configuration command. To disable the NetBIOS name-caching function, use the **no** form of this command.

**source-bridge proxy-netbios-only**

**no source-bridge proxy-netbios-only**

---

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

## source-bridge ring-group

To define or remove a ring group from the configuration, use the **source-bridge ring-group** global configuration command. To cancel previous assignments, use the **no** form of this command.

**source-bridge ring-group** *ring-group* [*virtual-mac-address*]

**no source-bridge ring-group** *ring-group* [*virtual-mac-address*]

<b>Syntax Description</b>	<i>ring-group</i>	Ring group number. The valid range is 1 to 4095.
	<i>virtual-mac-address</i>	(Optional) 12-digit hexadecimal string written as a dotted triple of four-digit hexadecimal numbers (for example, 0010.0a00.20a6).

## source-bridge route-cache

To enable fast switching, use the **source-bridge route-cache** interface configuration command. To disable fast switching, use the **no** form of this command.

**source-bridge route-cache**

**no source-bridge route-cache**

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

## source-bridge route-cache cbus

To enable autonomous switching, use the **source-bridge route-cache cbus** interface configuration command. To disable autonomous switching, use the **no** form of this command.

**source-bridge route-cache cbus**

**no source-bridge route-cache cbus**

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

## source-bridge route-cache sse

To enable the Cisco silicon switching engine (SSE) switching function, use the **source-bridge route-cache sse** interface configuration command. To disable SSE switching, use the **no** form of this command.

```
source-bridge route-cache sse
```

```
no source-bridge route-cache sse
```

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

## source-bridge sap-80d5

To allow non-IBM hosts (attached to a router with 80d5 processing enabled) to use the standard Token Ring to Ethernet LLC2 translation instead of the nonstandard Token Ring to Ethernet 80d5 translation, use the **source-bridge sap-80d5** global configuration command. This command allows you to set the translation on a per-DSAP basis. To disable this feature, use the **no** form of this command.

```
source-bridge sap-80d5 dsap
```

```
no source-bridge sap-80d5 dsap
```

**Syntax Description** *dsap* Destination service access point (DSAP).

## source-bridge spanning (automatic)

To enable the automatic spanning-tree function for a specified group of bridged interfaces, use the automatic version of the **source-bridge spanning** interface configuration command. To return to the default disabled state, use the **no** form of this command. To return an assigned path cost to the default path cost of 16, use the **no source-bridge spanning path-cost** command.

```
source-bridge spanning bridge-group [path-cost path-cost]
```

```
no source-bridge spanning bridge-group [path-cost path-cost]
```

<b>Syntax Description</b>	<i>bridge-group</i>	Number in the range 1 to 9 that you choose to refer to a particular group of bridged interfaces. This must be the same number as assigned in the <b>bridge protocol ibm</b> command.
	<b>path-cost</b>	(Optional) Assign a path cost for a specified interface.
	<i>path-cost</i>	(Optional) Path cost for the interface. The valid range is 0 to 65535.

## source-bridge spanning (manual)

To enable use of spanning explorers, use the **source-bridge spanning** interface configuration command. To disable the use of spanning explorers, use the **no** form of this command. Only spanning explorers will be blocked; everything else will be forwarded.

**source-bridge spanning**

**no source-bridge spanning**

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

## source-bridge transparent

To establish bridging between transparent bridging and source-route bridging (SRB), use the **source-bridge transparent** global configuration command. To disable a previously established link between a source-bridge ring group and a transparent bridge group, use the **no** form of this command.

**source-bridge transparent** *ring-group pseudoring bridge-number tb-group [oui]*

**no source-bridge transparent** *ring-group pseudoring bridge-number tb-group*

<b>Syntax Description</b>	<i>ring-group</i>	Virtual ring group created by the <b>source-bridge ring-group</b> command. This is the source-bridge virtual ring to associate with the transparent bridge group. This ring group number must match the number you have specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.
	<i>pseudoring</i>	Ring number used to represent the transparent bridging domain to the source-route bridged domain. This number must be a unique number, not used by any other ring in your source-route bridged network.
	<i>bridge-number</i>	Bridge number of the bridge that leads to the transparent bridging domain.
	<i>tb-group</i>	Number of the transparent bridge group that you want to tie into your source-route bridged domain. The <b>no</b> form of this command disables this feature.
	<i>oui</i>	(Optional) Organizational unique identifier. Possible values include the following: <ul style="list-style-type: none"> <li>• <b>90-compatible</b></li> <li>• <b>standard</b></li> <li>• <b>cisco</b></li> </ul>

# source-bridge transparent fastswitch

To enable fast switching of packets between the SRB and transparent domains, use the **source-bridge transparent fastswitch** global configuration command. To disable fast switching of packets, use the **no** form of this command.

**source-bridge transparent *ring-group* fastswitch**

**no source-bridge transparent *ring-group* fastswitch**

---

**Syntax Description**

---

*ring-group*

Virtual ring group created by the **source-bridge ring-group** command. This is the source-bridge virtual ring to associate with the transparent bridge group. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 to 4095.

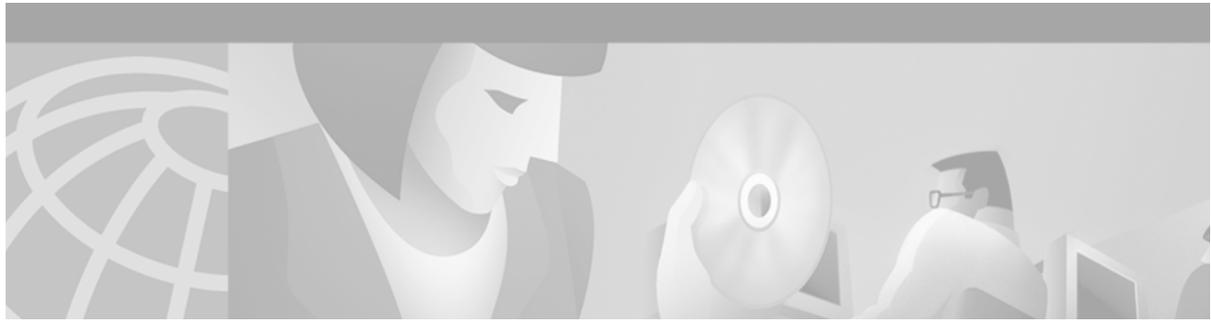
---

**fastswitch**

Fast-switched SR/TLB enables the Cisco IOS software to process packets at the interrupt level.

---

■ source-bridge transparent fastswitch



## Token Ring Inter-Switch Link Commands

---

This chapter describes the function and syntax of the Token Ring Inter-Switch Link (TRISL) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### clear drip counters

To clear duplicate ring protocol (DRiP) counters, use the **clear drip counters** privileged EXEC command.

**clear drip counters**

---

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

### encapsulation tr-isl trbrf-vlan

To enable TRISL, a Cisco protocol for interconnecting multiple routers and switches and maintaining Token Ring VLAN information as traffic goes between switches, use the **encapsulation tr-isl trbrf-vlan** subinterface configuration command. To disable the TRISL configuration, use the **no** form of this command.

**encapsulation tr-isl trbrf-vlan** *vlanid* **bridge-num** *bridge-number*

**no encapsulation tr-isl trbrf-vlan** *vlanid* **bridge-num** *bridge-number*

---

<b>Syntax Description</b>	<i>vlanid</i>	Number identifying the VLAN.
	<b>bridge-num</b> <i>bridge-number</i>	Keyword and bridge number assigned to the ISL trunk. Possible values are 01 to 15.

---

## multiring trcrf-vlan

To create a pseudoring to terminate the RIF for source-routed traffic and assign it to a VLAN, use the **multiring trcrf-vlan** interface configuration command. To disable the caching of RIFs on the subinterface, use the **no** form of this command.

**multiring trcrf-vlan** *vlanid* **ring** *ring-number*

**no multiring trcrf-vlan** *vlanid* **ring** *ring-number*

### Syntax Description

<i>vlanid</i>	VLAN ID number.
<b>ring</b> <i>ring-number</i>	Keyword and the logical ring number for Token Ring VLANs. Possible values are 01 to 4095.

## show drip

To display the status of the DRiP database, use the **show drip** privileged EXEC command.

**show drip**

### Syntax Description

This command has no arguments or keywords.

## source-bridge trcrf-vlan

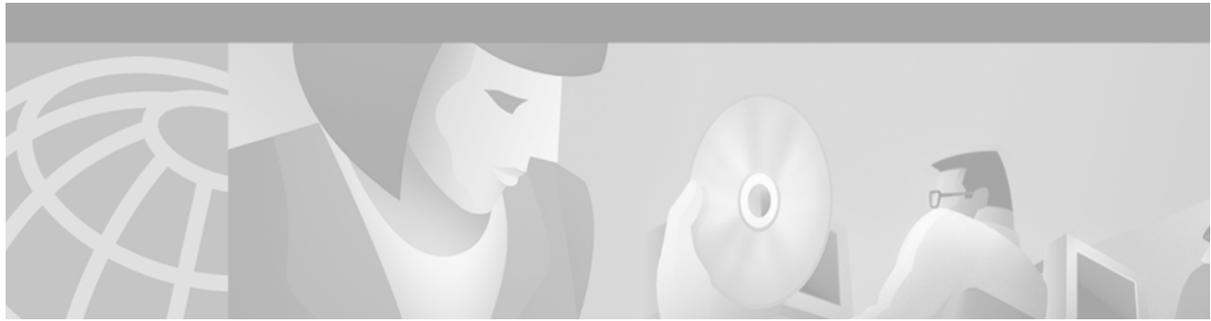
To attach a TrCRF VLAN to the router's virtual ring, use the **source-bridge trcrf-vlan** privileged EXEC command. To disable the attachment of a VLAN to the router's virtual ring, use the **no** form of this command.

**source-bridge trcrf-vlan** *vlanid* **ring-group** *ringnum*

**no source-bridge trcrf-vlan** *vlanid* **ring-group** *ringnum*

### Syntax Description

<i>vlanid</i>	VLAN ID number.
<b>ring-group</b> <i>ringnum</i>	Keyword and ring number of the virtual ring.



## Token Ring Route Switch Module Commands

---

This chapter describes the function and syntax of the Token Ring Route Switch Module commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### clear drip counters

To clear duplicate ring protocol (DRiP) counters from the RSM interfaces, use the **clear drip counters** privileged EXEC command.

```
clear drip counters
```

---

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

### interface vlan

To configure a Token Ring or Ethernet interface on the RSM, use the **interface vlan** interface configuration command.

```
interface vlan vlanid type { trbrf | ethernet }
```

---

<b>Syntax Description</b>	<i>vlanid</i>	Unique VLAN ID number used to create a VLAN.
	<b>type trbrf</b>	Configures a Token Ring interface on the RSM.
	<b>type ethernet</b>	Configures an Ethernet interface on the RSM.

---

## multiring trcrf-vlan

To create a pseudoring on the RSM and to terminate the RIF when routing IP or IPX source-routed traffic on Token Ring VLAN (TrBRF) interfaces, use the **multiring trcrf-vlan** interface configuration command. To disable the termination of RIFs on the RSM interface, use the **no** form of this command.

**multiring trcrf-vlan** *vlanid* **ring-group** *ring-number*

**no multiring trcrf-vlan** *vlanid* **ring-group** *ring-number*

### Syntax Description

<i>vlanid</i>	VLAN ID number. Valid VLAN ID numbers are 2 through 1000.
<b>ring-group</b> <i>ring-number</i>	Keyword that specifies the pseudoring number used to terminate the RIF.

## show drip

To display the status of the DRiP database for a router or an RSM, use the **show drip** privileged EXEC command.

**show drip**

### Syntax Description

This command has no arguments or keywords.

## source-bridge trcrf-vlan

To attach a VLAN to the RSM's virtual ring when source-route bridging, use the **source-bridge trcrf-vlan** interface configuration command. To disable the attachment of a VLAN to the RSM's virtual ring, use the **no** form of this command.

**source-bridge trcrf-vlan** *vlanid* **ring-group** *ringnum*

### Syntax Description

<i>vlanid</i>	VLAN ID number.
<b>ring-group</b> <i>ringnum</i>	Pseudoring number that corresponds to the virtual ring number for the interface.



## Remote Source-Route Bridging Commands

---

This chapter describes the function and syntax of the remote source-route bridging (RSRB) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### locaddr-priority

To assign a remote source-route bridging (RSRB) priority group to an input interface, use the **locaddr-priority** interface configuration command. To remove the RSRB priority group assignment from the interface, use the **no** form of this command.

**locaddr-priority** *list-number*

**no locaddr-priority** *list-number*

---

#### Syntax Description

*list-number*

Priority list number of the input interface.

---

### locaddr-priority-list

To map logical units (LUs) to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses, use the **locaddr-priority-list** global configuration command. To remove that priority queueing assignment, use the **no** form of this command. You use this command in conjunction with the **priority list** command.

**locaddr-priority-list** *list-number address-number queue-keyword [dsap ds] [dmac dm] [ssap ss] [smac sm]*

**no locaddr-priority-list** *list-number address-number queue-keyword [dsap ds] [dmac dm] [ssap ss] [smac sm]*

---

#### Syntax Description

*list-number*

Arbitrary integer between 1 and 10 that identifies the LU address priority list selected by the user.

*address-number*

Value of the LOCADDR= parameter on the LU macro, which is a one-byte address of the LU in hexadecimal.

---

<i>queue-keyword</i>	Enables a priority queue type: Valid queue-keyword values and their equivalent priority queue type level are: <ul style="list-style-type: none"> <li>• <b>high</b>—Priority queue type is high.</li> <li>• <b>medium</b>—Priority queue type is medium.</li> <li>• <b>normal</b>—Priority queue type is normal.</li> <li>• <b>low</b>—Priority queue type is low.</li> </ul>
<b>dsap</b> <i>ds</i>	(Optional) Indicates that the next argument, <i>ds</i> , represents the destination service access point address. The argument <i>ds</i> is a hexadecimal value.
<b>dmac</b> <i>dm</i>	(Optional) Indicates that the next argument, <i>dm</i> , is the destination MAC address. The argument <i>dm</i> is written as a dotted triple of four-digit hexadecimal numbers.
<b>ssap</b> <i>ss</i>	(Optional) Indicates that the next argument, <i>ss</i> , is the source service access point address. If this is not specified, the default is all source service access point addresses.
<b>smac</b> <i>sm</i>	(Optional) Indicates that the next argument, <i>sm</i> , is the source MAC address, written as a dotted triple of four-digit hexadecimal numbers. If this is not specified, the default is all source MAC addresses.

## priority-list protocol

To establish queueing priorities based upon the protocol type as one of the steps to establishing queueing priorities based on logical unit (LU) addresses, use the **priority-list protocol** global configuration command. To remove the priority list, use the **no** form of this command.

**priority-list** *list-number protocol protocol-name queue-keyword*

**no priority-list** *list-number protocol protocol-name queue-keyword*

### Syntax Description

<i>list-number</i>	Arbitrary integer between 1 and 10 that identifies the LU address priority list selected by the user.
<i>protocol-name</i>	Protocol you are using. In most cases, this will be <b>ip</b> .
<i>queue-keyword</i>	Priority queue name; one of <b>high</b> , <b>medium</b> , <b>normal</b> , or <b>low</b> .

## rsrb remote-peer lsap-output-list

To define service access point (SAP) filters by local SAP (LSAP) address on the remote source-route bridging WAN interface, use the **rsrb remote-peer lsap-output-list** global configuration command. To remove a SAP filter on the RSRB WAN interface, use the **no** form of this command.

**rsrb remote-peer** *ring-group {tcp ip-address | fst ip-address | interface name} lsap-output-list access-list-number*

**no rsrb remote-peer** *ring-group {tcp ip-address | fst ip-address | interface name} lsap-output-list access-list-number*

<b>Syntax Description</b>	<i>ring-group</i>	Virtual ring number of the remote peer.
	<b>tcp</b>	TCP encapsulation.
	<b>fst</b>	FST encapsulation.
	<i>ip-address</i>	IP address.
	<b>interface</b>	Direct encapsulation.
	<i>name</i>	Interface name.
	<i>access-list-number</i>	Number of the access list.

## rsrb remote-peer netbios-output-list

To filter packets by NetBIOS station name on a remote source-route bridging WAN interface, use the **rsrb remote-peer netbios-output-list** global configuration command. To remove a filter on an RSRB WAN interface, use the **no** form of this command.

```
rsrb remote-peer ring-group {tcp ip-address | fst ip-address | interface type} netbios-output-list
host name
```

```
no rsrb remote-peer ring-group {tcp ip-address | fst ip-address | interface type}
netbios-output-list host name
```

<b>Syntax Description</b>	<i>ring-group</i>	Virtual ring number of the remote peer.
	<b>tcp</b>	TCP encapsulation.
	<b>fst</b>	FST encapsulation.
	<i>ip-address</i>	IP address.
	<b>interface</b>	Direct encapsulation.
	<i>type</i>	Interface name.
	<i>name</i>	Name of a NetBIOS access filter previously defined with one or more <b>netbios access-list host</b> global configuration commands.

## sap-priority

To define a priority list on an interface, use the **sap-priority** interface configuration command. To remove a priority list on an interface, use the **no** form of this command.

```
sap-priority list-number
```

```
no sap-priority list number
```

<b>Syntax Description</b>	<i>list-number</i>	Priority list number you specified in the <b>sap-priority-list</b> command.
---------------------------	--------------------	---

## sap-priority-list

To define a priority list, use the **sap-priority-list** global configuration command. To remove a priority list, use the **no** form of this command.

**sap-priority-list** *list-number queue-keyword* [**dsap** *ds*] [**ssap** *ss*] [**dmac** *dm*] [**smac** *sm*]

**no sap-priority-list** *list-number queue-keyword* [**dsap** *ds*] [**ssap** *ss*] [**dmac** *dm*] [**smac** *sm*]

Syntax Description		
	<i>list-number</i>	Arbitrary integer between 1 and 10 that identifies the priority list.
	<i>queue-keyword</i>	Priority queue name or a remote source-route bridge TCP port name.
	<b>dsap</b> <i>ds</i>	(Optional) Destination service access point address. The argument <i>ds</i> is a hexadecimal number.
	<b>ssap</b> <i>ss</i>	(Optional) Source service access point address. The argument <i>ss</i> is a hexadecimal number.
	<b>dmac</b> <i>dm</i>	(Optional) Destination MAC address. The argument <i>dm</i> is written as a dotted triple of four-digit hexadecimal numbers.
	<b>smac</b> <i>sm</i>	(Optional) Source MAC address. The argument <i>sm</i> is written as a dotted triple of four-digit hexadecimal numbers.

## show local-ack

To display the current state of any current local acknowledgment for both LLC2 and SDLLC connections, and for any configured passthrough rings, use the **show local-ack** privileged EXEC command.

**show local-ack**

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

## source-bridge cos-enable

To force the Cisco IOS software to read the contents of the format identification (FID) frames to prioritize traffic when using TCP, use the **source-bridge cos-enable** global configuration command. To disable prioritizing, use the **no** form of this command.

**source-bridge cos-enable**

**no source-bridge cos-enable**

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

## source-bridge fst-peername

To set up a Fast-Sequenced Transport (FST) peer name, use the **source-bridge fst-peername** global configuration command. To disable the IP address assignment, use the **no** form of this command.

**source-bridge fst-peername** *local-interface-address*

**no source-bridge fst-peername** *local-interface-address*

---

### Syntax Description

*local-interface-address*

IP address to assign to the local router.

---

## source-bridge keepalive

To assign the keepalive interval of the remote source-bridging peer, use the **source-bridge keepalive** interface configuration command. To cancel previous assignments, use the **no** form of this command.

**source-bridge keepalive** *seconds*

**no source-bridge keepalive**

---

### Syntax Description

*seconds*

Keepalive interval in seconds. The valid range is 10 to 300. The default value is 30 seconds.

---

## source-bridge largest-frame

To configure the largest frame size that is used to communicate with any peers in the ring group, use the **source-bridge largest-frame** global configuration command. To cancel previous assignments, use the **no** form of this command.

**source-bridge largest-frame** *ring-group size*

**no source-bridge largest-frame** *ring-group*

---

### Syntax Description

*ring-group*

Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 to 4095.

*size*

Maximum frame size. The default is that no frame size is assigned.

---

## source-bridge passthrough

To configure some sessions on a few rings to be locally acknowledged and the remaining to passthrough, use the **source-bridge passthrough** global configuration command. To disable passthrough on all the rings and allow the session to be locally acknowledged, use the **no** form of this command.

**source-bridge passthrough** *ring-group*

**no source-bridge passthrough** *ring-group*

<b>Syntax Description</b>	<i>ring-group</i>	Ring group number. This ring is either the start ring or destination ring of the two IBM end machines for which the passthrough feature is to be configured. This ring group number must match the number you specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.
---------------------------	-------------------	---

## source-bridge remote-peer frame-relay

To specify a point-to-point direct encapsulation connection, use the **source-bridge remote-peer frame-relay** global configuration command. To disable previous interface assignments, use the **no** form of this command.

**source-bridge remote-peer** *ring-group* **frame-relay interface** *name* [*mac-address*] [*dldci-number*]  
[*if size*]

**no source-bridge remote-peer** *ring-group* **frame-relay interface** *name*

<b>Syntax Description</b>	<i>ring-group</i>	Ring group number. This ring group number must match the number you specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.
	<b>interface</b> <i>name</i>	Name of the interface over which to send source-route bridged traffic.
	<i>mac-address</i>	(Optional) MAC address for the interface on the other side of the virtual ring. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the <b>show interface</b> command, and then scanning the display for the interface specified by <i>name</i> .
	<i>dldci-number</i>	(Optional) Data-link connection identifier (DLCI) number for Frame Relay encapsulation.
	<b>if</b> <i>size</i>	(Optional) Maximum-sized frame to be sent to this remote peer. The Cisco IOS software negotiates all transit routes down to this size or lower. This argument is useful in preventing timeouts in end hosts by reducing the amount of data they have to send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407 and 17800 bytes.

## source-bridge remote-peer fst

To specify a Fast-Sequenced Transport (FST) encapsulation connection, use the **source-bridge remote-peer fst** global configuration command. To disable the previous assignments, use the **no** form of this command.

```
source-bridge remote-peer ring-group fst ip-address [if size]
```

```
no source-bridge remote-peer ring-group fst ip-address
```

Syntax Description		
	<i>ring-group</i>	Ring group number. This ring group number must match the number you specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.
	<i>ip-address</i>	IP address of the remote peer with which the router will communicate.
	<b>if size</b>	(Optional) Maximum-sized frame to be sent to this remote peer. The Cisco IOS software negotiates all transit routes down to this size or lower. Use this argument to prevent timeouts in end hosts by reducing the amount of data they have to send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

## source-bridge remote-peer tcp

To identify the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP, use the **source-bridge remote-peer tcp** global configuration command. To remove a remote peer for the specified ring group, use the **no** form of this command.

```
source-bridge remote-peer ring-group tcp ip-address [if size] [tcp-receive-window wsize]
[local-ack] [priority]
```

```
no source-bridge remote-peer ring-group tcp ip-address
```

Syntax Description		
	<i>ring-group</i>	Ring group number. This ring group number must match the number you specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.
	<i>ip-address</i>	IP address of the remote peer with which the router will communicate. The default is that no IP address is identified.
	<b>if size</b>	(Optional) Maximum-sized frame to be sent to this remote peer. The Cisco IOS software negotiates all transit routes down to this size or lower. Use this argument to prevent timeouts in end hosts by reducing the amount of data they have to send in a fixed interval. The valid values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.
	<b>tcp-receive-window wsize</b>	(Optional) The TCP receive window size in bytes. The range is 10240 to 65535 bytes. The default window size is 10240 bytes.

<b>local-ack</b>	(Optional) LLC2 sessions destined for a specific remote peer are locally terminated and acknowledged. Use local acknowledgment for LLC2 sessions going to this remote peer.
<b>priority</b>	(Optional) Enables prioritization over a TCP network. You must specify the keyword <b>local-ack</b> earlier in the same <b>source-bridge remote-peer</b> command. The keyword <b>priority</b> is a prerequisite for features such as System Network Architecture (SNA) class of service and SNA LU address prioritization over a TCP network.

## source-bridge tcp-queue-max

To modify the size of the backup queue for remote source-route bridging, use the **source-bridge tcp-queue-max** global configuration command. This backup queue determines the number of packets that can wait for transmission to a remote ring before packets start being thrown away. To return to the default value, use the **no** form of this command.

**source-bridge tcp-queue-max** *number*

**no source-bridge tcp-queue-max**

### Syntax Description

<i>number</i>	Number of packets to hold in any single outgoing TCP queue to a remote router. The default is 100 packets.
---------------	--



## DLSw+ Commands

---

This chapter describes the function and syntax of the data-link switching plus (DLSw+) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### clear dlsw circuit

To cause all DLSw+ circuits to be closed, use the **clear dlsw circuit** privileged EXEC command.

```
clear dlsw circuit [circuit-id]
```

---

**Syntax Description**

*circuit-id*      Circuit ID for a specific remote circuit. The valid range is 0 to 4294967295.

---

### clear dlsw reachability

To remove all entries from the DLSw+ reachability cache, use the **clear dlsw reachability** privileged EXEC command.

```
clear dlsw reachability
```

---

**Syntax Description**

This command has no arguments or keywords.

### clear dlsw statistics

To reset to zero the number of frames that have been processed in the local, remote, and group cache, use the **clear dlsw statistics** privileged EXEC command.

```
clear dlsw statistics
```

---

**Syntax Description**

This command has no arguments or keywords.

## dlsw allroute-netbios

To change the single-route explorer to an all-route broadcast for NetBIOS, use the **dlsw allroute-netbios** global configuration command. To return to the default single-route explorer, use the **no** form of this command.

**dlsw allroute-netbios**

**no dlsw allroute-netbios**

---

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

## dlsw allroute-sna

To change the single-route explorer to an all-route broadcast for SNA, use the **dlsw allroute-sna** global configuration command. To return to the default single-route explorer, use the **no** form of this command.

**dlsw allroute-sna**

**no dlsw allroute-sna**

---

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

## dlsw bgroup-list

To map traffic on the local Ethernet bridge group interface to remote peers, use the **dlsw bgroup-list** global configuration command. To cancel the map, use the **no** form of this command.

**dlsw bgroup-list** *list-number* **bgroups** *number*

**no dlsw bgroup-list**

---

<b>Syntax Description</b>	<i>list-number</i>	The ring list number. This number is subsequently used in the <b>dlsw remote-peer</b> command to define the segment to which the bridge group should be applied. The valid range is 1 to 255.
	<b>bgroups</b> <i>number</i>	The transparent bridge group list number. The valid range is 1 to 63.

---

# dlsw bridge-group

To link DLSw+ to the bridge group of the Ethernet LANs, use the **dlsw bridge-group** global configuration command. To disable the link, use the **no** form of this command.

```
dlsw bridge-group group-number [llc2 [N2 number] [ack-delay-time milliseconds]
[ack-max number] [idle-time milliseconds] [local-window number] [t1-time milliseconds]
[tbusy-time milliseconds] [tpf-time milliseconds] [trej-time milliseconds]
[txq-max number] [xid-neg-val-time milliseconds] [xid-retry-time milliseconds]
[locaddr-priority lu address priority list number] [sap-priority priority list number]
```

```
no dlsw bridge-group group-number [llc2 [N2 number] [ack-delay-time milliseconds]
[ack-max number] [idle-time milliseconds] [local-window number] [t1-time milliseconds]
[tbusy-time milliseconds] [tpf-time milliseconds] [trej-time milliseconds]
[txq-max number] [xid-neg-val-time milliseconds] [xid-retry-time milliseconds]
[locaddr-priority lu address priority list number] [sap-priority priority list number]
```

Syntax Description	
<i>group-number</i>	Transparent bridge group to which DLSw+ will be attached. The valid range is 1 to 63.
<b>llc2</b>	(Optional) LLC2 interface subcommands.
<b>N2 number</b>	(Optional) Number of times router should retry various operations. The valid range is 1 to 255.
<b>ack-delay-time</b> <i>milliseconds</i>	(Optional) Maximum time the router allows incoming I-frames to stay unacknowledged. The valid range is 1 to 60000.
<b>ack-max</b> <i>number</i>	(Optional) Maximum number of I-frames received before an acknowledgment must be sent. The valid range is 1 to 255.
<b>idle-time</b> <i>milliseconds</i>	(Optional) Frequency of polls during periods of idle traffic. The valid range is 1 to 60000.
<b>local-window</b> <i>number</i>	(Optional) Maximum number of I-frames to send before waiting for an acknowledgment. The valid range is 1 to 127.
<b>t1-time</b> <i>milliseconds</i>	(Optional) Amount of time router waits for an acknowledgment to sent I-frames. The valid range is 1 to 60000.
<b>tbusy-time</b> <i>milliseconds</i>	(Optional) Amount of time router waits while the other LLC2 station is in a busy state before attempting to poll the remote station. The valid range is 1 to 60000.
<b>tpf-time</b> <i>milliseconds</i>	(Optional) Amount of time router waits for a final response to a poll frame before re-sending the original poll frame. The valid range is 1 to 60000.
<b>trej-time</b> <i>milliseconds</i>	(Optional) Amount of time router waits for a resend of a rejected frame before sending the reject command. The valid range is 1 to 60000.
<b>txq-max</b> <i>number</i>	(Optional) Queue for holding LLC2 information frames. The valid range is 20 to 200.
<b>xid-neg-val-time</b> <i>milliseconds</i>	(Optional) Frequency of exchange of identification (XID). The valid range is 1 to 60000.
<b>xid-retry-time</b> <i>milliseconds</i>	(Optional) Amount of time router waits for reply to XID. The valid range is 1 to 60000.

<b>locaddr-priority</b> <i>lu address priority list number</i>	(Optional) Assigns an input SNA LU Addr priority list to this bridge group. The valid range is 1 to 10.
<b>sap-priority</b> <i>priority list number</i>	(Optional) Assigns an input sap priority list to this bridge group. The valid range is 1 to 10.

## dlsw cache-ignore-netbios-datagram

To prevent DLSw from caching NetBIOS names when a datagram (0x08) NetBIOS command is received, use the **dlsw cache-ignore-netbios-datagram** global configuration command. To remove the filter, use the **no** form of this command.

**dlsw cache-ignore-netbios-datagram**

**no dlsw cache-ignore-netbios-datagram**

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

## dlsw disable

To disable DLSw+ without altering the configuration, use the **dlsw disable** global configuration command. To reenable DLSw+, use the **no** form of this command.

**dlsw disable**

**no dlsw disable**

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

## dlsw duplicate-path-bias

To specify how DLSw+ handles duplicate paths to the same Media Access Control (MAC) address or NetBIOS name, use the **dlsw duplicate-path-bias** global configuration command. To return to the default (fault-tolerance), use the **no** form of this command.

**dlsw duplicate-path-bias** [**load-balance**]

**no dlsw duplicate-path-bias** [**load-balance**]

**Syntax Description** **load-balance** (Optional) Specifies that sessions are load-balanced across duplicate paths.

## dlsw explorerq-depth

To establish queue depth for multiple queues that handle various types of explorer traffic, including SNA and NetBIOS frames, use the **dlsw explorerq-depth** global configuration command. To remove the queues, use the **no** form of this command.

**dlsw explorerq-depth** { *sna value* | *netbios value* | **other value** }

**no dlsw explorerq-depth** { *sna value* | *netbios value* | **other value** }

Syntax Description		
	<b>sna value</b>	Establishes queue depth for SNA frames. The valid range is from 10 to 1000. The default is unlimited.
	<b>netbios value</b>	Establishes queue depth for NetBIOS frames. The valid range is from 10 to 1000. The default is unlimited.
	<b>other value</b>	Establishes queue depth for unnumbered information (UI) frames. The valid range is from 10 to 1000. The default 100.

## dlsw group-cache disable

To disable the border peer caching feature, use the **dlsw group-cache disable** global configuration command. To return to the default peer caching feature, use the **no** form of this command.

**dlsw group-cache disable**

**no dlsw group-cache disable**

Syntax Description	
	This command has no arguments or keywords.

## dlsw group-cache max-entries

To limit the number of entries in the group cache, use the **dlsw group-cache max entries** global configuration command. To return to the default, use the **no** form of this command.

**dlsw group-cache max-entries** *number*

**no dlsw group-cache max entries**

Syntax Description		
	<i>number</i>	Maximum number of entries allowed in the group cache. The valid range is 0 through 12000. If the value is set to 0, then there is no limit to the number of entries. The default is 2000.

## dlsw icannotreach saps

To configure a list of service access points (SAPs) not locally reachable by the router, use the **dlsw icannotreach saps** global configuration command. To remove the list, use the **no** form of this command.

```
dlsw icannotreach saps sap...
```

```
no dlsw icannotreach saps sap...
```

### Syntax Description

---

<i>sap...</i>	One or more SAPs, separated by spaces.
---------------	--

---

## dlsw icanreach

To configure a resource that is locally reachable by this router, use the **dlsw icanreach** global configuration command. To remove the resource, use the **no** form of this command.

```
dlsw icanreach { mac-exclusive | netbios-exclusive [remote] | mac-address mac-addr [mask mask] | netbios-name name | saps }
```

```
no dlsw icanreach { mac-exclusive | netbios-exclusive [remote] | mac-address mac-addr [mask mask] | netbios-name name | saps }
```

### Syntax Description

---

<b>mac-exclusive</b>	Router can reach only the MAC addresses that are user configured.
<b>netbios-exclusive</b>	Router can reach only the NetBIOS names that are user configured.
<b>remote</b>	(Optional) Gives the NetBIOS workstations (that are local to the router and that are not already defined in the <b>dlsw icanreach netbios-name name</b> statement) access to remote servers.
<b>mac-address</b> <i>mac-addr</i>	Configures a MAC address that this router can locally reach.
<b>mask</b> <i>mask</i>	(Optional) MAC address mask in hexadecimal <i>h.h.h</i> . The “F” value represents the “care” bit and the “0” value represents the “don’t care” bit. The mask indicates which bits in the MAC address are relevant.
<b>netbios-name</b> <i>name</i>	Configures a NetBIOS name that this router can locally reach. Wildcards (*) are allowed at the end of the name. Trailing white spaces are ignored when comparing against an actual name in a NetBIOS frame.
<b>saps</b>	Array of SAPs.

---

## dlsw llc2 nornr

To prevent the receiver not ready (RNR) message from being sent while establishing an LLC2 connection, use the **dlsw llc2 nornr** global configuration command. To return to the default, use the **no** form of this command.

**dlsw llc2 nornr**

**no dlsw llc2 nornr**

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

## dlsw load-balance

To enable load balancing and to select either round robin or circuit-count-based load balancing, use the **dlsw load-balance** global configuration command. To disable the previous assignments, use the **no** form of this command.

**dlsw load-balance** [**round-robin** | **circuit-count** *circuit weight*]

**no dlsw load-balance** [**round-robin** | **circuit-count** *circuit weight*]

Syntax Description		
<b>round-robin</b>	(Optional)	Enables round-robin type of load balancing.
<b>circuit-count</b> <i>circuit weight</i>	(Optional)	Enables the DLSw+ Enhanced Load Balancing feature. The value represents the default circuit weight to be used for the peers that are not explicitly configured with a circuit-weight value in the <b>dlsw remote-peer tcp</b> command. The valid range is 1 to 100.

## dlsw local-peer

To define the parameters of the DLSw+ local peer, use the **dlsw local-peer** global configuration command. To cancel the definitions, use the **no** form of this command.

**dlsw local-peer** [**cluster** *cluster-id*] [**peer-id** *ip-address*] [**group** *group*] [**border**] [**cost** *cost*] [**If size**] [**keepalive** *seconds*] [**passive**] [**promiscuous**] [**biu-segment**] [**init-pacing-window** *size*] [**max-pacing-window** *size*]

**no dlsw local-peer** [**cluster** *cluster-id*] [**peer-id** *ip-address*] [**group** *group*] [**border**] [**cost** *cost*] [**If size**] [**keepalive** *seconds*] [**passive**] [**promiscuous**] [**biu-segment**] [**init-pacing-window** *size*] [**max-pacing-window** *size*]

Syntax Description		
<b>cluster</b> <i>cluster-id</i>	(Optional)	Implements the DLSw+ Peer Clusters feature and defines the router as part of a particular cluster. The valid range is 1 to 255.
<b>peer-id</b> <i>ip-address</i>	(Optional)	Local peer IP address. This address is required when Fast-Sequenced Transport (FST) or TCP is used.

<b>group</b> <i>group</i>	(Optional) Peer group number for this router. The valid range is 1 to 255.
<b>border</b>	(Optional) Enables the router as a border peer. The group option must be specified to use the border peer option.
<b>cost</b> <i>cost</i>	(Optional) Peer cost advertised to remote peers in the capabilities exchange. The valid range is 1 to 5.
<b>if</b> <i>size</i>	(Optional) Largest frame size for this local peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
<b>keepalive</b> <i>seconds</i>	(Optional) Default remote peer keepalive interval in seconds. The valid range is 0 to 1200 seconds. The default is 30 seconds. The value 0 means no keepalives.
<b>passive</b>	(Optional) Specifies that this router does not initiate remote peer connections to configured peers.
<b>promiscuous</b>	(Optional) Accept connections from nonconfigured remote peers.
<b>biu-segment</b>	(Optional) DLSw+ spoofs the maximum receivable I-frame size in XID so that each end station sends its largest frame.
<b>init-pacing-window</b> <i>size</i>	(Optional) Size of the initial pacing window as defined in RFC 1795. The valid range is 1 to 2000.
<b>max-pacing-window</b> <i>size</i>	(Optional) Maximum size of the pacing window as defined in RFC 1795. The valid range is 1 to 2000.

## dlsw mac-addr

To configure a static MAC address, use the **dlsw mac-addr** global configuration command. To cancel the configuration, use the **no** form of this command.

```
dlsw mac-addr mac-addr { ring ring-number | remote-peer { interface serial number | ip-address ip-address } | rif rif-string | group group }
```

```
no dlsw mac-addr mac-addr { ring ring-number | remote-peer { interface serial number | ip-address ip-address } | rif rif-string | group group }
```

### Syntax Description

<i>mac-addr</i>	Specifies the MAC address.
<b>ring</b> <i>ring-number</i>	Maps the MAC address to a ring number or ring group number. The valid range is 1 to 4095.
<b>remote-peer</b>	Maps the MAC address to a specific remote peer.
<b>interface serial</b> <i>number</i>	Specifies the remote peer by direct serial interface.
<b>ip-address</b> <i>ip-address</i>	Specifies the remote peer by IP address.
<b>rif</b> <i>rif-string</i>	Maps the MAC address to a local interface using a RIF string. The RIF string describes a source-routed path from the router to the MAC address. It starts at the router's ring-group and ends on the ring where the MAC address is located. The direction should be from the router toward the MAC address. See IEEE 802.5 standard for details.
<b>group</b> <i>group</i>	Maps the MAC address to a specified peer group. Valid numbers are in the range 1 to 255.

## dlsw max-multiple-rifs

To enable caching of multiple RIFs per interface, use the **dlsw max-multiple-rifs** global configuration command. To turn off the feature, use the **no** form of this command.

```
dlsw max-multiple-rifs multiple-rifs-per-port
```

```
no dlsw max-multiple-rifs multiple-rifs-per-port
```

<b>Syntax Description</b>	<i>multiple-rifs-per-port</i>	Number of multiple RIF entries per interface. The valid range is 1 to 4. The default value is 1.
---------------------------	-------------------------------	--

## dlsw netbios-keepalive-filter

To enable the NetBIOS dial-on-demand routing (DDR) feature, use the **dlsw netbios-keepalive-filter** global configuration command. To turn off the feature, use the **no** form of this command.

```
dlsw netbios-keepalive-filter
```

```
no dlsw netbios-keepalive-filter
```

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

## dlsw netbios-name

To configure a static NetBIOS name, use the **dlsw netbios-name** global configuration command. To cancel the configuration, use the **no** form of this command.

```
dlsw netbios-name netbios-name {ring ring-number | remote-peer {interface serial number | ip-address ip-address}} | rif rif-string | group group}
```

```
no dlsw netbios-name netbios-name {ring ring-number | remote-peer {interface serial number | ip-address ip-address}} | rif rif-string | group group}
```

<b>Syntax Description</b>	<i>netbios-name</i>	Specifies the NetBIOS name. Wildcards are allowed.
	<b>ring</b> <i>ring number</i>	Maps the NetBIOS name to a ring number or ring group number. Test frames for this name will only be sent to LAN ports in this ring group.
	<b>remote-peer</b>	Maps the NetBIOS name to a specific remote peer.
	<b>interface serial</b> <i>number</i>	Specifies the remote peer by direct interface.
	<b>ip-address</b> <i>ip-address</i>	Specifies the remote peer by IP address.

<b>rif</b> <i>rif-string</i>	Maps the MAC address to a local interface using a RIF string. The RIF string describes a source-routed path from the router to the MAC address, starting at the router's ring-group and ending on the ring where the MAC address is located. The direction is from the router towards the MAC address. See the IEEE 802.5 standard for details.
<b>group</b> <i>group</i>	Maps the NetBIOS name to a specified peer group. Valid numbers are in the range 1 to 255.

## dlsw peer-on-demand-defaults

To configure defaults for peer-on-demand transport, use the **dlsw peer-on-demand-defaults** global configuration command. To disable the previous assignment, use the **no** form of this command.

```
dlsw peer-on-demand-defaults [fst] [bytes-netbios-out bytes-list-name] [cost cost] [dest-mac
destination-mac-address] [dmac-output-list access-list-number] [host-netbios-out
host-list-name] [inactivity minutes] [keepalive seconds] [if size] [lsap-output-list list]
[port-list port-list-number] [priority] [rsvp {global | average-bit-rate maximum burst}]
[tcp-queue-max]
```

```
no dlsw peer-on-demand-defaults [fst] [bytes-netbios-out bytes-list-name] [cost cost] [dest-mac
destination-mac-address] [dmac-output-list access-list-number] [host-netbios-out
host-list-name] [inactivity minutes] [keepalive seconds] [if size] [lsap-output-list list]
[port-list port-list-number] [priority] [rsvp {global | average-bit-rate maximum burst}]
[tcp-queue-max]
```

### Syntax Description

<b>fst</b>	(Optional) Use FST encapsulation for all peers-on-demand established by this router.
<b>bytes-netbios-out</b> <i>bytes-list-name</i>	(Optional) Configures NetBIOS bytes output filtering for peer-on-demand peers. The <i>bytes-list-name</i> is the name of the previously defined NetBIOS bytes access list filter.
<b>cost</b> <i>cost</i>	(Optional) Specifies the cost to reach peer-on-demand peer. The valid range is 1 to 5. The default cost is 3.
<b>dest-mac</b> <i>destination-mac-address</i>	(Optional) Specifies the exclusive destination MAC address for peer-on-demand peers.
<b>dmac-output-list</b> <i>access-list-number</i>	(Optional) Specifies the filter output destination MAC addresses.
<b>host-netbios-out</b> <i>host-list-name</i>	(Optional) Configures NetBIOS host output filtering for peer-on-demand peers. The <i>host-list-name</i> is the name of the previously defined NetBIOS host access list filter.
<b>inactivity</b> <i>minutes</i>	(Optional) Configures the length of time after the peer's circuit count is 0 that the peer-on-demand is disconnected. The valid range is 0 to 1440 seconds. The default is 600 seconds.
<b>keepalive</b> <i>seconds</i>	(Optional) Configures the peer-on-demand keepalive interval. The valid range is 0 to 1200 seconds. The default is 30 seconds.

<b>lf size</b>	(Optional) Largest frame size for this remote peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
<b>lsap-output-list list</b>	(Optional) Configures local service access point (LSAP) output filtering for peer-on-demand peers. Valid numbers are in the range 200 to 299.
<b>port-list port-list-number</b>	(Optional) Configures a port list for peer-on-demand peers. Valid numbers are in the range 0 to 4095.
<b>priority</b>	(Optional) Configures prioritization for peer-on-demand peers. The default state is off.
<b>rsvp global</b>	(Optional) Sets the RSVP parameters to the global values specified in the <b>dlsw rsvp</b> command.
<b>rsvp average-bit-rate</b>	(Optional) Average bit rate kilobits per second to reserve up to 75 percent of total bits on the interface. The valid range is 0 to 4294967.
<b>maximum-burst</b>	(Optional) Maximum burst size (kilobytes of data in queue). The valid range is 0 to 4294967.
<b>tcp-queue-max</b>	(Optional) Configures the maximum output TCP queue size for peer-on-demand peers.

## dlsw port-list

To map traffic on a local interface (Token Ring or serial) to remote peers, use the **dlsw port-list** global configuration command. To disable the previous map assignment, use the **no** form of this command.

**dlsw port-list** *list-number type number*

**no dlsw port-list** *list-number type number*

### Syntax Description

<i>list-number</i>	Port list number. The valid range is 1 to 255.
<i>type</i>	Interface type.
<i>number</i>	Interface number.

## dlsw prom-peer-defaults

To configure defaults for promiscuous transport, use the **dlsw prom-peer-defaults** global configuration command. To disable the previous assignment, use the **no** form of this command.

```
dlsw prom-peer-defaults [fst] [bytes-netbios-out bytes-list-name] [cost cost] [dest-mac
destination-mac-address] [dmac-output-list access-list-number] [host-netbios-out
host-list-name] [keepalive seconds] [lf size] [lsap-output-list list] [rsvp {global | learn |
average-bit-rate maximum burst}] [tcp-queue-max size]
```

```
no dlsw prom-peer-defaults [fst] [bytes-netbios-out bytes-list-name] [cost cost] [dest-mac
destination-mac-address] [dmac-output-list access-list-number] [host-netbios-out
host-list-name] [keepalive seconds] [lf size] [lsap-output-list list] [rsvp {global | learn |
average-bit-rate maximum burst}] [tcp-queue-max size]
```

Syntax Description	
<b>fst</b>	(Optional) Use FST encapsulation for all promiscuous peers established by this router.
<b>bytes-netbios-out</b> <i>bytes-list-name</i>	(Optional) Configures NetBIOS bytes output filtering for promiscuous peers. The <i>bytes-list-name</i> is the name of the previously defined NetBIOS bytes access list filter.
<b>cost</b> <i>cost</i>	(Optional) Specifies the cost to reach promiscuous peers. The valid range is 1 to 5. The default cost is 3.
<b>dest-mac</b> <i>destination-mac-address</i>	(Optional) Specifies the exclusive destination MAC address for promiscuous peers.
<b>dmac-output-list</b> <i>access-list-number</i>	(Optional) Specifies the filter output destination MAC addresses.
<b>host-netbios-out</b> <i>host-list-name</i>	(Optional) Configures NetBIOS host output filtering for promiscuous peers. The <i>host-list-name</i> is the name of the previously defined NetBIOS host access list filter.
<b>keepalive</b> <i>seconds</i>	(Optional) Configures the promiscuous keepalive interval. The valid range is 0 to 1200 seconds. The default is 30 seconds.
<b>lf</b> <i>size</i>	(Optional) Largest frame size for this promiscuous peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
<b>lsap-output-list</b> <i>list</i>	(Optional) Configures LSAP output filtering for promiscuous peers. Valid numbers are 200 to 299.
<b>rsvp global</b>	(Optional) Sets the RSVP parameters to the global values.
<b>rsvp learn</b>	(Optional) Configures RSVP parameters ( <i>average-bit-rate</i> and <i>maximum burst</i> rate) to be those of the remote peer to which the promiscuous peer is connecting.
<i>average-bit-rate</i>	(Optional) Configures RSVP parameters for this peer connection, which are different from the global values. Average bit rate (kilobits per second) to reserve up to 75 percent of the total bits on the interface. The valid range is 0 to 4294967.

<i>maximum-burst</i>	(Optional) Maximum burst size (kilobytes of data in queue). The valid range is 0 to 4294967.
<b>tcp-queue-max</b> <i>size</i>	(Optional) Configures the maximum output TCP queue size for promiscuous peers.

## dlsw redundant-rings

To eliminate caching problems and explorer looping when multiple DLSw+ peers are connected to a single Token Ring LAN where the virtual ring numbers configured in those DLSw+ routers are different, use the **dlsw redundant-rings** global configuration command. To disable the previous settings, use the **no** form of this command.

```
dlsw redundant-rings [ring]...
```

```
no dlsw redundant-rings [ring]...
```

<b>Syntax Description</b>	<i>ring</i>	(Optional) Virtual ring number. You can configure up to 10 redundant rings, separated by spaces.
---------------------------	-------------	--

## dlsw remote-peer frame-relay

To specify the remote peer with which the router will connect, use the **dlsw remote-peer frame-relay** global configuration command. To disable the previous assignments, use the **no** form of this command.

```
dlsw remote-peer list-number frame-relay interface serial number dlci-number [backup-peer
[ip-address | frame-relay interface serial number dlci-number | interface name |
circuit-inactivity minutes]] [bytes-netbios-out bytes-list-name] [circuit-weight weight] [cost
cost] [dest-mac mac-address] [dmac-output-list access-list-number]
[host-netbios-out host-list-name] [keepalive seconds] [lf size] [linger minutes]
[lsap-output-list list] [passive] pass-thru
```

```
no dlsw remote-peer list-number frame-relay interface serial number dlci-number
[backup-peer [ip-address | frame-relay interface serial number dlci-number |
interface name | circuit-inactivity minutes]] [bytes-netbios-out bytes-list-name]
[circuit-weight weight] [cost cost] [dest-mac mac-address]
[dmac-output-list access-list-number] [host-netbios-out host-list-name]
[keepalive seconds] [lf size] [linger minutes] [lsap-output-list list] [passive] pass-thru
```

<b>Syntax Description</b>	<i>list-number</i>	Ring list number. The valid range is 1 to 255. The default is 0, which means DLSw+ forwards explorers over all ports or bridge groups on which DLSw+ is enabled.
	<b>interface serial</b> <i>number</i>	Serial interface number of the remote peer with which the router is to communicate.
	<i>dlci-number</i>	DLCI number of the remote peer.
	<b>backup-peer</b> <i>ip-address</i>	(Optional) IP address of the existing TCP/FST peer for which this peer is the backup peer.

<b>backup-peer frame-relay interface serial</b> <i>number</i> <i>dcli-number</i>	(Optional) Serial interface and DLCI number of the existing Direct/LLC2 Frame-Relay peer for which this peer is the backup peer.
<b>backup-peer interface</b> <i>name</i>	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
<b>backup-peer circuit-inactivity</b> <i>minutes</i>	(Optional) Configures the length of time a circuit is inactive before being terminated. May be used with the <code>linger</code> option. The valid range is 1 to 1440 minutes.
<b>bytes-netbios-out</b> <i>bytes-list-name</i>	(Optional) Configures NetBIOS bytes output filtering for this peer. The <i>bytes-list-name</i> argument is the name of the previously defined NetBIOS bytes access list filter.
<b>circuit weight</b> <i>weight</i>	(Optional) Configures circuit weight for this remote peer.
<b>cost</b> <i>cost</i>	(Optional) Cost to reach this remote peer. The valid range is 1 to 5.
<b>dest-mac</b> <i>mac-address</i>	(Optional) Permits the connection to be established only when there is an explorer frame destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
<b>dmac-output-list</b> <i>access-list-number</i>	(Optional) Establishes the connection only when the explorer frame passes the specified access list. The <i>access-list-number</i> is the list number specified in the <b>access-list</b> command.
<b>host-netbios-out</b> <i>host-list-name</i>	(Optional) Configures NetBIOS host output filtering for this peer. The <i>host-list-name</i> is the name of the previously defined NetBIOS host access list filter.
<b>keepalive</b> <i>seconds</i>	(Optional) Sets the keepalive interval for this remote peer. The range is 0 to 1200 seconds.
<b>if</b> <i>size</i>	(Optional) Largest frame size, in bytes, this local peer will use on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
<b>linger</b> <i>minutes</i>	(Optional) Configures length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is 1 to 300 minutes. The default is 5 minutes.
<b>lsap-output-list</b> <i>list</i>	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 to 299.
<b>passive</b>	(Optional) Designates this remote peer as passive.
<b>pass-thru</b>	(Optional) Selects passthrough mode. The default is local acknowledgement mode.

## dlsw remote-peer fst

To specify an FST encapsulation connection for remote peer transport, use the **dlsw remote-peer fst** global configuration command. To disable the previous FST assignments, use the **no** form of this command.

**dlsw remote-peer** *list-number* **fst** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dcli-number* | **interface** *name*]] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lfr** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**]

**no dlsw remote-peer** *list-number* **fst** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dcli-number* | **interface** *name*]] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lfr** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**]

Syntax Description		
<i>list-number</i>		Ring list number. The valid range is 1 to 255. The default is 0, which means DLSw+ forwards explorers over all ports or bridge groups on which DLSw+ is enabled.
<i>ip-address</i>		IP address of the remote peer with which the router is to communicate.
<b>backup-peer</b> <i>ip-address</i>		(Optional) IP address of the existing TCP/FST peer for which this peer is the backup peer.
<b>backup-peer</b> <b>frame-relay-interface serial</b> <i>number dcli-number</i>		(Optional) Serial interface and DLCI number of the existing Direct/LLC2 Frame Relay peer for which this peer is the backup peer.
<b>backup-peer</b> <i>interface name</i>		(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
<b>bytes-netbios-out</b> <i>bytes-list-name</i>		(Optional) Configures NetBIOS bytes output filtering for this peer. The <i>bytes-list-name</i> argument is the name of the previously defined NetBIOS bytes access list filter.
<b>cost</b> <i>cost</i>		(Optional) Cost to reach this remote peer. The valid range is 1 to 5.
<b>dest-mac</b> <i>mac-address</i>		(Optional) Permits the connection to be established only when there is an explorer frame destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
<b>dmac-output-list</b> <i>access-list-number</i>		(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The <i>access-list-number</i> is the list number specified in the <b>access-list</b> command.
<b>host-netbios-out</b> <i>host-list-name</i>		(Optional) Configures NetBIOS host output filtering for this peer. The <i>host-list-name</i> is the name of the previously defined NetBIOS host access list filter.
<b>keepalive</b> <i>seconds</i>		(Optional) Sets the keepalive interval for this remote peer. The range is 0 to 1200 seconds.

<b>lf size</b>	(Optional) Largest frame size this local peer will use on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
<b>linger minutes</b>	(Optional) Configures length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is 1 to 300 minutes. The default is 5 minutes.
<b>lsap-output-list list</b>	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 to 299.
<b>passive</b>	(Optional) Designates this remote peer as passive.

## dlsw remote-peer interface

To specify a point-to-point direct encapsulation connection, use the **dlsw remote-peer interface** global configuration command. To disable previous interface assignments, use the **no** form of this command.

**dlsw remote-peer list-number interface serial number [backup-peer [ip-address | frame-relay interface serial number dlci-number | interface name | circuit-inactivity minutes]] [bytes-netbios-out bytes-list-name] [cost cost] [dest-mac mac-address] [dmac-output-list access-list-number] [host-netbios-out host-list-name] [keepalive seconds] [lf size] [linger minutes] [lsap-output-list list] [passive] [pass-thru]**

**no dlsw remote-peer list-number interface serial number [backup-peer [ip-address | frame-relay interface serial number dlci-number | interface name | circuit-inactivity minutes]] [bytes-netbios-out bytes-list-name] [cost cost] [dest-mac mac-address] [dmac-output-list access-list-number] [host-netbios-out host-list-name] [keepalive seconds] [lf size] [linger minutes] [lsap-output-list list] [passive] [pass-thru]**

### Syntax Description

<b>list-number</b>	Ring list number. The valid range is 1 to 255. The default is 0, which means all.
<b>serial number</b>	Specifies the remote peer by direct serial interface.
<b>backup-peer ip-address</b>	(Optional) IP address of the existing TCP/FST peer for which this peer is the backup peer.
<b>backup-peer frame-relay interface serial number dlci-number</b>	(Optional) Serial interface and DLCI number of the existing Direct/LLC2 frame-relay peer for which this peer is the backup peer.
<b>backup-peer interface name</b>	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
<b>backup-peer circuit-inactivity minutes</b>	(Optional) Configures the length of time a circuit is inactive before being terminated. May be used with the linger option. The valid range is 1 to 1440 minutes.
<b>bytes-netbios-out bytes-list-name</b>	(Optional) Configures NetBIOS bytes output filtering for this peer. The <i>bytes-list-name</i> argument is the name of the previously defined NetBIOS bytes access list filter.
<b>cost cost</b>	(Optional) Cost to reach this remote peer. The valid range is 1 to 5.

<b>dest-mac</b> <i>mac-address</i>	(Optional) Permits the connection to be established only when there is an explorer frame destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
<b>dmac-output-list</b> <i>access-list-number</i>	(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The <i>access-list-number</i> is the list number specified in the <b>access-list</b> command.
<b>host-netbios-out</b> <i>host-list-name</i>	(Optional) Configures NetBIOS host output filtering for this peer. The <i>host-list-name</i> is the name of the previously defined NetBIOS host access list filter.
<b>keepalive</b> <i>seconds</i>	(Optional) Sets the keepalive interval for this remote peer. The range is 0 to 1200 seconds.
<b>lf</b> <i>size</i>	(Optional) Largest frame size, in bytes, this local peer will use on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
<b>linger</b> <i>minutes</i>	(Optional) Configures length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is 1 to 300 minutes. The default is 5 minutes.
<b>lsap-output-list</b> <i>list</i>	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 to 299.
<b>passive</b>	(Optional) Designates this remote peer as passive.
<b>pass-thru</b>	(Optional) Selects passthrough mode. The default is local acknowledgment mode.

## dlsw remote-peer tcp

To identify the IP address of a peer with which to exchange traffic using TCP, use the **dlsw remote-peer tcp** global configuration command. To remove a remote peer, use the **no** form of this command.

```
dlsw remote-peer list-number tcp ip-address [backup-peer [ip-address | frame-relay interface serial number dlc-number | interface name | circuit-inactivity minutes]] [bytes-netbios-out bytes-list-name] [cluster cluster-id] [circuit-weight value] [cost cost] [dest-mac mac-address] [dmac-output-list access-list-number] [dynamic] [host-netbios-out host-list-name] [inactivity minutes] [dynamic] [keepalive seconds] [lf size] [linger minutes] [lsap-output-list list] [no-llc minutes] [passive] [priority] [rif-passthru virtual-ring-number] [rsvp {global | average-bit-rate maximum burst}] [tcp-queue-max size] [timeout seconds]
```

```
no dlsw remote-peer list-number tcp ip-address [backup-peer [ip-address | frame-relay interface serial number dlc-number | interface name | circuit-inactivity minutes]] [bytes-netbios-out bytes-list-name] [cluster cluster-id] [circuit-weight value] [cost cost] [dest-mac mac-address] [dmac-output-list access-list-number] [dynamic] [host-netbios-out host-list-name] [inactivity minutes] [dynamic] [keepalive seconds] [lf size] [linger minutes] [lsap-output-list list] [no-llc minutes] [passive] [priority] [rif-passthru virtual-ring-number] [rsvp {global | average-bit-rate maximum burst}] [tcp-queue-max size] [timeout seconds]
```

## Syntax Description

<i>list-number</i>	Remote peer ring group list number. This ring group list number default is 0. Otherwise, this value must match the number you specify with the <b>dlsw ring-list</b> , <b>dlsw port-list</b> , or <b>dlsw bgroup-list</b> command.
<i>ip-address</i>	IP address of the remote peer with which the router is to communicate.
<b>backup-peer</b> <i>ip-address</i>	(Optional) IP address of the existing TCP/FST peer for which this peer is the backup peer.
<b>backup-peer frame-relay interface</b> <i>serial number</i> <i>dcli-number</i>	(Optional) Serial interface and DLCI number of the existing Direct/LLC2 Frame Relay peer for which this peer is the backup peer.
<b>backup-peer interface</b> <i>name</i>	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
<b>backup-peer circuit-inactivity</b> <i>minutes</i>	(Optional) Configures the length of time a circuit is idle before terminating the circuit. The valid range is 1 to 1440.
<b>bytes-netbios-out</b> <i>bytes-list-name</i>	(Optional) Configures NetBIOS bytes output filtering for this peer. The <i>bytes-list-name</i> argument is the name of the previously defined NetBIOS bytes access list filter.
<b>cluster</b> <i>cluster-id</i>	(Optional) Used to indicate to a border peer that a particular remote-peer should be treated as part of a specific peer cluster. The valid Range is 1 to 255.
<b>circuit-weight</b> <i>value</i>	(Optional) Configures the target state that DLSw+ tries to maintain. The valid range is 1 to 100.
<b>cost</b> <i>cost</i>	(Optional) Cost to reach this remote peer. The valid range is 1 to 5.
<b>dest-mac</b> <i>mac-address</i>	(Optional) Specifies the exclusive 48-bit destination MAC address, written as a dotted triple of four-digit hexadecimal numbers, for peer-on-demand peers.  If the <b>dynamic</b> keyword is also specified, the TCP connection is established only when there is an explorer frame destined for the specified MAC address.
<b>dmac-output-list</b> <i>access-list-number</i>	(Optional) Specifies the filter output destination MAC addresses. The <i>access-list-number</i> is the list number specified in an <b>access-list</b> command.  If the <b>dynamic</b> keyword is also specified, the TCP connection is established only when the explorer frame passes the specified access list.
<b>dynamic</b>	(Optional) Establishes the TCP connection only when there is DLSw+ data to send.
<b>host-netbios-out</b> <i>host-list-name</i>	(Optional) Configures NetBIOS host output filtering for this peer. The <i>host-list-name</i> is the name of the previously defined NetBIOS host access list filter.
<b>inactivity</b> <i>minutes</i>	(Optional) Configures the length of time a connection is idle before closing the dynamic remote peer connection. The valid range is 1 to 300 minutes. The default is 5 minutes.
<b>keepalive</b> <i>seconds</i>	(Optional) Sets the keepalive interval for this remote peer. The range is 0 to 1200 seconds.

<b>if size</b>	(Optional) Largest frame size, in bytes, this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
<b>linger minutes</b>	(Optional) Configures length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is 1 to 300 minutes. The default is 5 minutes.
<b>lsap-output-list list</b>	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 to 299.
<b>no-llc minutes</b>	(Optional) Configures the length of time a remote peer remains connected after all LLC2 connections are gone. The valid range is 1 to 300 minutes. The default is 5 minutes.
<b>passive</b>	(Optional) Designates this remote peer as passive.
<b>priority</b>	(Optional) Enables prioritization features for this remote peer. Valid TCP port numbers are the following: <ul style="list-style-type: none"> <li>• High—2065</li> <li>• Medium—1981</li> <li>• Normal—1982</li> <li>• Low—1983</li> </ul>
<b>rif-passthru virtual-ring-number</b>	(Optional) Configures the remote peer as RIF-Passthru. The <i>virtual-ring-number</i> value is the same number as the <i>ring number</i> value assigned in the <b>source-bridge ring-group</b> commands of the DLSw+ Passthru peers.
<b>rsvp global</b>	(Optional) Configures the RSVP parameters for this specific peer back to the global values.
<b>rsvp average-bit-rate</b>	(Optional) Configures RSVP parameters for this peer, which are different from the global values. Average bit rate (kilobits per second) reserves up to 75 percent of the total bits on the interface. Range is 0 to 4294967.
<b>maximum burst</b>	(Optional) Maximum burst size (kilobytes of data in queue). Range is 0 to 4294967.
<b>tcp-queue-max size</b>	(Optional) Maximum output TCP queue size for this remote peer. The valid maximum TCP queue size is a number in the range 10 to 2000.
<b>timeout seconds</b>	(Optional) Resend time limit for TCP. The valid range is 5 to 1200 seconds. The default is 90 seconds.

## dlsw ring-list

To configure a ring list, mapping traffic on a local interface to remote peers, use the **dlsw ring-list** global configuration command. To cancel the definition, use the **no** form of this command.

**dlsw ring-list** *list-number* **rings** *ring-number*

**no dlsw ring-list** *list-number* **rings** *ring-number*

**Syntax Description**

<i>list-number</i>	Ring list number. The valid range is 1 to 255.
<b>rings</b>	Specify one or more physical or virtual rings.
<i>ring-number</i>	Physical or virtual ring number. The valid range is 1 to 4095.

## dlsw rsvp

To enable the DLSw+ RSVP Bandwidth Reservation feature on the local peer, use the **dlsw rsvp** global configuration command. To disable the DLSw+ RSVP Bandwidth Reservation feature for all peers in the router, use the **no** form of this command.

```
dlsw rsvp { default | [average-bit-rate maximum-burst] }
```

```
no dlsw rsvp { default | [average-bit-rate maximum-burst] }
```

**Syntax Description**

<b>default</b>	Sets the average bit rate to 10 kbps and the maximum burst rate to 28 kbps.
<i>average-bit-rate</i>	(Optional) Average bit rate (kilobits per second) to reserve up to 75 percent of the total bits on the interface. The valid range is 1 to 4294967 kbps.
<i>maximum-burst</i>	(Optional) Maximum burst size (kilobytes of data in queue). The valid range is 1 to 4294967 kbps.

## dlsw timer

To tune an existing configuration parameter, use the **dlsw timer** global configuration command. To restore the default parameters, use the **no** form of this command.

```
dlsw timer { icannotreach-block-time | netbios-cache-timeout | netbios-explorer-timeout |  
netbios-group-cache | netbios-retry-interval | netbios-verify-interval | sna-cache-timeout |  
explorer-delay-time | sna-explorer-timeout | explorer-wait-time | sna-group-cache |  
sna-retry-interval | sna-verify-interval } time
```

```
no dlsw timer { icannotreach-block-time | netbios-cache-timeout | netbios-explorer-timeout |  
netbios-group-cache | netbios-retry-interval | netbios-verify-interval | sna-cache-timeout |  
explorer-delay-time | sna-explorer-timeout | explorer-wait-time | sna-group-cache |  
sna-retry-interval | sna-verify-interval } time
```

**Syntax Description**

<b>icannotreach-block-time</b>	Cache life of unreachable resource; during this time searches for the resource are blocked. The valid range is 1 to 86400 seconds. The default is 0 (disabled).
<b>netbios-cache-timeout</b>	Cache life of NetBIOS name location for the local and remote reachability caches. The valid range is 1 to 86400 seconds. The default is 960 seconds (16 minutes).
<b>netbios-explorer-timeout</b>	Length of time that the Cisco IOS software waits for an explorer response before marking a resource unreachable (on both a LAN and a WAN). The valid range is 1 to 86400 seconds. The default is 6 seconds.

<b>netbios-group-cache</b>	Cache life of NetBIOS entries in the group cache. The valid range is 1 to 86000 seconds. The default is 240 seconds (4 minutes).
<b>netbios-retry-interval</b>	NetBIOS explorer retry interval (on a LAN only). The valid range is 1 to 86400 seconds. The default is 1 second.
<b>netbios-verify-interval</b>	Number of seconds between a cache entry's creation and its marking as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to ensure the cache still exists. The valid range is 1 to 86400 seconds. The default is 240 seconds (4 minutes).
<b>sna-cache-timeout</b>	Length of time that an SNA MAC/service access point (SAP) location cache entry exists before it is discarded (for local and remote caches). The valid range is 1 to 86400 seconds. The default is 960 seconds (16 minutes).
<b>explorer-delay-time</b>	Time to wait before sending or accepting explorers. The valid range is 1 to 5 minutes. The default is 0.
<b>sna-explorer-timeout</b>	Length of time that the Cisco IOS software waits for an explorer response before marking a resource unreachable (on a LAN and WAN). The valid range is 1 to 86400 seconds. The default is 180 seconds (3 minutes).
<b>explorer-wait-time</b>	Time to wait for all stations to respond to explorers. The valid range is 1 to 86400 seconds. The default is 0.
<b>sna-group-cache</b>	Cache life of SNA entries in the group cache. The valid range is 1 to 86000 seconds. The default is 240 seconds (4 minutes).
<b>sna-retry-interval</b>	Interval between SNA explorer retries (on a LAN). The valid range is 1 to 86400 seconds. The default is 30 seconds.
<b>sna-verify-interval</b>	Number of seconds between a cache entry's creation and its marking as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to ensure that the cache still exists. The valid range is 1 to 86400 seconds. The default is 240 seconds (4 minutes).
<i>time</i>	Length of time for selected timer, in seconds.

## dlsw tos disable

To disable any ToS bits in DLSw+ generated packets, use the **dlsw tos disable** global configuration command. To return to the default, use the **no** form of this command.

**dlsw tos disable**

**no dlsw tos disable**

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

## dlsw tos map

To associate a ToS value for priority peers, use the **dlsw tos map** global configuration command. To return to the default, use the **no** form of this command.

```
dlsw tos map [high value [medium value | normal value | low value]]
```

```
no dlsw tos map [high value [medium value | normal value | low value]]
```

Syntax Description		
<b>high</b> <i>value</i>	(Optional) Overrides the default values set for the port labeled “high.” The value is the ToS bit value. Valid range is 0 to 7.	
<b>medium</b> <i>value</i>	(Optional) Overrides the default values set for the port labeled “medium.” The value is the ToS bit value. Valid range is 0 to 7.	
<b>normal</b> <i>value</i>	(Optional) Overrides the default values set for the port labeled “normal.” The value is the ToS bit value. Valid range is 0 to 7.	
<b>low</b> <i>value</i>	(Optional) Overrides the default values set for the port labeled “low.” The value is the ToS bit value. Valid range is 0 to 7.	

## dlsw transparent map

To enable MAC address mapping in a switch-based environment, use the **dlsw transparent map** interface configuration command. To disable MAC address mapping, use the **no** form of this command.

```
dlsw transparent map local mac mac address remote mac mac address [neighbor mac address]
```

```
no dlsw transparent map local mac mac address remote mac mac address  
[neighbor mac address]
```

Syntax Description		
<b>local mac</b> <i>mac address</i>	MAC address that is created and given to the remote device. This MAC address is mapped to the actual MAC address that is specified in the <b>remote mac</b> <i>mac address</i> option.	
<b>remote mac</b> <i>mac address</i>	MAC address of the remote device.	
<b>neighbor</b> <i>mac address</i>	(Optional) MAC address of the DLSw+ device that takes over mapping if the primary DLSw+ device becomes unavailable.	

## dlsw transparent redundancy-enable

To configure transparent redundancy, use the **dlsw transparent redundancy-enable** interface configuration command. To disable transparent redundancy, use the **no** form of this command.

```
dlsw transparent redundancy-enable multicast-mac-address [master-priority value]
```

```
no dlsw transparent redundancy-enable multicast-mac-address [master-priority value]
```

<b>Syntax Description</b>	<i>multicast-mac-address</i>	MAC address to which all DLSw+ devices on a transparent bridged domain advertise their presence by sending the master present frame.
	<b>master-priority</b> <i>value</i>	(Optional) Configures the router as a master device. The valid range is 0 to 254. The lower the value, higher the priority. The default value is 100.

## dlsw transparent switch-support

To enable the special support that is required for the interfaces connected to an Ethernet switch with the **dlsw transparent redundancy-enable** command configured, use the **dlsw transparent switch-support** global configuration command. To disable DLSW transparent switch support, use the **no** form of this command.

```
dlsw transparent switch-support
```

```
no dlsw transparent switch-support
```

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

## dlsw transparent timers

To configure the timeout value the master router waits for all requests for a circuit before giving the permission for a router for a circuit, use the **dlsw transparent timers** interface configuration command. To disable the timeout value, use the **no** form of this command.

```
dlsw transparent timers [netbios value | sna value]
```

```
no dlsw transparent timers [netbios value | sna value]
```

<b>Syntax Description</b>	<b>netbios</b> <i>value</i>	(Optional) Timeout value for the NetBIOS session. The valid range is 100 to 900 ms. The default value is 400 ms.
	<b>sna</b> <i>value</i>	(Optional) Timeout value for the SNA session. The valid range is 100 to 5000 ms. The default value is 1000 ms (1 second).

## dlsw udp-disable

To disable the UDP unicast feature, use the **dlsw udp-disable** global configuration command. To return to the default UDP unicast feature, use the **no** form of this command.

```
dlsw udp-disable
```

```
no dlsw udp-disable
```

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

## qlc dlsw

To enable DLSw+ over Qualified Logical Link Control (QLLC), use the **qlc dlsw** interface configuration command. To cancel the configuration, use the **no** form of this command.

```
qlc dlsw {subaddress subaddress | pvc pvc-low [pvc-high]} [vmac vmacaddr poolsize] [partner
partner-macaddr] [sap ssap dsap] [xid xidstring] [npsi-poll]
```

```
no qlc dlsw {subaddress subaddress | pvc pvc-low [pvc-high]} [vmac vmacaddr poolsize]
[partner partner-macaddr] [sap ssap dsap] [xid xidstring] [npsi-poll]
```

### Syntax Description

<b>subaddress</b> <i>subaddress</i>	An X.121 subaddress.
<b>pvc</b>	Map one or more permanent virtual circuits (PVCs) to a particular QLLC service (in this case DLSw+). QLLC will attempt to reach the partner by sending and ID.STN.IND to DLSw+.
<i>pvc-low</i>	Lowest logical channel number (LCN) for a range of X.25 PVCs. Acceptable values for PVCs are decimal numbers between 1 and 4095.
<i>pvc-high</i>	(Optional) Highest LCN. If not specified the range of PVCs consists of just one PVC.
<b>vmac</b> <i>vmacaddr</i>	(Optional) Defines either the only virtual MAC address used for DLSw+ or the lowest virtual MAC address in a pool of virtual MAC addresses.
<i>poolsize</i>	(Optional) Specify the number of contiguous virtual MAC addresses that have been reserved for DLSw+. If the parameter is not present, then just one virtual MAC address is available.
<b>partner</b> <i>partner-macaddr</i>	(Optional) Virtual MAC address to which an incoming call wishes to connect. The <b>qlc dlsw</b> command must be repeated for each different partner. Each partner is identified by a unique subaddress.
<b>sap</b> <i>ssap dsap</i>	(Optional) Overrides the default SAP values (04) for a Token Ring connection. <i>dsap</i> refers to the partner's SAP address; <i>ssap</i> applies to the virtual MAC address that corresponds to the X.121 device.
<b>xid</b> <i>xidstring</i>	(Optional) XID format 0 type 2 string.
<b>npsi-poll</b>	(Optional) Inhibits forwarding a null XID on the X.25 link. Instead the Cisco IOS software will send a null XID response back to the device that sent the null XID command.

## sdlc dlsw

To attach SDLC addresses to DLSw+, use the **sdlc dlsw** interface configuration command. To cancel the configuration, use the **no** form of this command.

```
sdlc dlsw {sdlc-address | default | partner mac-address [inbound | outbound]}
```

```
no sdlc dlsw {sdlc-address | default | partner mac-address [inbound | outbound]}
```

<b>Syntax Description</b>	<i>sdlc-address</i>	SDLC addresses are in hexadecimal. The valid range is 1 to FE.
	<b>default</b>	Allows the user to configure an unlimited number of SDLC addresses to DLSw+.
	<b>partner</b> <i>mac-address</i>	MAC address for default partner
	<b>inbound</b>	(Optional) Partner will initiate connection.
	<b>outbound</b>	(Optional) Initiate connection to partner.

## show dlsw capabilities

To display the configuration of a specific peer or all peers, use the **show dlsw capabilities** privileged EXEC command.

```
show dlsw capabilities [interface type number | ip-address ip-address | local]
```

<b>Syntax Description</b>	<b>interface</b> <i>type number</i>	(Optional) Specifies the interface type and number for which the DLSw+ capabilities are to be displayed.
	<b>ip-address</b> <i>ip-address</i>	(Optional) Specifies a peer by its IP address.
	<b>local</b>	(Optional) Specifies the local DLSw+ peer.

## show dlsw circuits

To display the state of all circuits involving this MAC address as a source and destination, use the **show dlsw circuits** privileged EXEC command.

```
show dlsw circuits [detail] [mac-address address | sap-value value | circuit id]
```

<b>Syntax Description</b>	<b>detail</b>	(Optional) Display circuit state information in expanded format.
	<b>mac-address</b> <i>address</i>	(Optional) Specifies the MAC address to be used in the circuit search.
	<b>sap-value</b> <i>value</i>	(Optional) Specifies the SAP to be used in the circuit search.
	<b>circuit id</b>	(Optional) Specifies the circuit ID of the circuit index.

## show dlsw fastcache

To display the fast cache for FST and direct-encapsulated peers, use the **show dlsw fastcache** privileged EXEC command.

```
show dlsw fastcache
```

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

## show dlsw peers

To display DLSw peer information, use the **show dlsw peers** privileged EXEC command.

```
show dlsw peers [interface type number | ip-address ip-address | ssp-dlx [interface type number
| ip-address ip-address] | udp]
```

Syntax Description		
<b>interface</b> <i>type number</i>	(Optional)	Specifies a remote peer by a direct interface.
<b>ip-address</b> <i>ip-address</i>	(Optional)	Specifies a remote peer by its IP address.
<b>ssp-dlx</b>	(Optional)	Details SSP and DLX primitive frames received and sent by a TCP or LLC2 peer.
<b>udp</b>	(Optional)	Shows UDP frame forwarding statistics for specified peers.

## show dlsw reachability

To display DLSw+ reachability information, use the **show dlsw reachability** privileged EXEC command.

```
show dlsw reachability [[group [value] | local | remote] | [mac-address [address]
[netbios-names [name]]]
```

Syntax Description		
<b>group</b>	(Optional)	Displays contents of group reachability cache only.
<i>value</i>	(Optional)	Specifies the group number for the reachability check. Only displays group cache entries for the specified group. The valid range is 1 to 255.
<b>local</b>	(Optional)	Displays contents of local reachability cache only.
<b>remote</b>	(Optional)	Displays contents of remote reachability cache only.
<b>mac-address</b>	(Optional)	Displays DLSw reachability for MAC addresses only.
<i>address</i>	(Optional)	Specifies the MAC address for which to search in the reachability cache.
<b>netbios-names</b>	(Optional)	Displays DLSw reachability for NetBIOS names only.
<i>name</i>	(Optional)	Specifies the NetBIOS name for which to search in the reachability cache.

## show dlsw statistics

To display the number of frames that have been processed in the local, remote, and group cache, use the **show dlsw statistics** privileged EXEC command.

```
show dlsw statistics [border-peers]
```

Syntax Description		
<b>border-peers</b>	(Optional)	Displays the number of frames processed in the local, remote, and group caches.

## show dlsw transparent cache

To display the master circuit cache for each transparent bridged domain, use the **show dlsw transparent cache** privileged EXEC command.

```
show dlsw transparent cache
```

---

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

## show dlsw transparent map

To display MAC address mappings on the local router and any mappings for which the local router is acting as backup for a neighbor peer, use the **show dlsw transparent map** privileged EXEC command.

```
show dlsw transparent map
```

---

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

## show dlsw transparent neighbor

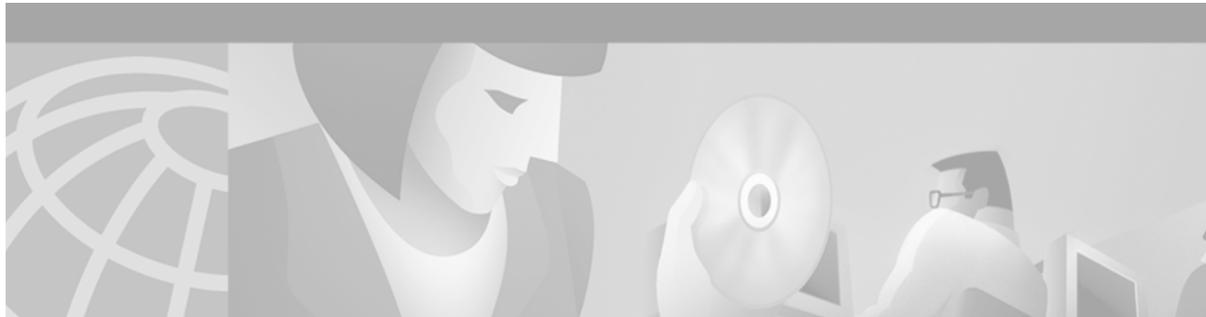
To display DLSw neighbors in a transparent bridged domain, use the **show dlsw transparent neighbor** privileged EXEC command.

```
show dlsw transparent neighbor
```

---

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

■ show dlsw transparent neighbor



## Serial Tunnel and Block Serial Tunnel Commands

---

This chapter describes the function and syntax of the serial tunnel (STUN) and block serial tunnel (BSTUN) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### asp addr-offset

To configure an asynchronous port to send and receive polled asynchronous traffic through a BSTUN tunnel, use the **asp addr-offset** interface configuration command. To cancel the specification, use the **no** form of this command.

```
asp addr-offset address-offset
```

```
no asp addr-offset
```

---

#### Syntax Description

<i>address-offset</i>	Location of the address byte within the polled asynchronous frame being received.
-----------------------	---

---

### asp role

To specify whether the router is acting as the primary end of the polled asynchronous link or as the secondary end of the polled asynchronous link connected to the serial interface and whether the attached remote device is a security alarm control station, use the **asp role** interface configuration command. To cancel the specification, use the **no** form of this command.

```
asp role { primary | secondary }
```

```
no asp role { primary | secondary }
```

---

#### Syntax Description

<b>primary</b>	Router is the primary end of the polled asynchronous link connected to the serial interface, and the attached remote devices are alarm panels.
<b>secondary</b>	Router is the secondary end of the polled asynchronous link connected to the serial interface, and the attached remote device is a security alarm control station.

---

## asp rx-ift

To specify a time period that, by expiring, signals the end of one frame being received and the start of the next, use the **asp rx-ift** interface configuration command. To cancel the specification, use the **no** form of this command.

**asp rx-ift** *interframe-timeout*

**no asp rx-ift**

<b>Syntax Description</b>	<i>interframe-timeout</i>	Number of milliseconds between the end of one frame being received and the start of the next frame. The default timeout value is 40 ms.
---------------------------	---------------------------	---

## bsc char-set

To specify the character set used by the Bisync support feature in this serial interface as either EBCDIC or ASCII, use the **bsc char-set** interface configuration command. To cancel the character set specification, use the **no** form of this command.

**bsc char-set** {*ascii* | *ebcdic*}

**no bsc char-set** {*ascii* | *ebcdic*}

<b>Syntax Description</b>	<i>ascii</i>	ASCII character set.
	<i>ebcdic</i>	EBCDIC character set. This character set is the default.

## bsc contention

To specify an address on a contention interface, use the **bsc contention** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc contention** *address*

**no bsc contention**

<b>Syntax Description</b>	<i>address</i>	Address assigned to contention interface. The range is 1 to 255. The default is 0x01.
---------------------------	----------------	---

## bsc dial-contention

To specify a router at the central site as a central router with dynamic allocation of serial interfaces, use the **bsc dial-contention** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc dial-contention** *time-out*

**no bsc dial-contention**

<b>Syntax Description</b>	<i>time-out</i>	Amount of time interface can sit idle before it is returned to the idle interface pool. The range is 2 to 30 seconds. The default is 5 seconds.
---------------------------	-----------------	---

## bsc host-timeout

To detect deactivation of devices at the host, use the **bsc host-timeout** interface configuration command. To cancel the configuration, use the **no** form of this command.

**bsc host-timeout** *interval*

**no bsc host-timeout** *interval*

<b>Syntax Description</b>	<i>interval</i>	Timeout interval within which a poll or select for a control unit must be received. If this interval expires, the remote router is sent a teardown peer signal. The range is 30 to 3000 deciseconds. The default is 600 deciseconds (60 seconds).
---------------------------	-----------------	---

## bsc pause

To specify the interval, to the tenth of a second, between starts of the polling cycle, use the **bsc pause** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc pause** *time*

**no bsc pause** *time*

<b>Syntax Description</b>	<i>time</i>	Interval in tenths of a second. The default value is 10 (that is, 10 tenths of a second, or 1 second). The maximum time is 255 tenths of a second (25.5 seconds).
---------------------------	-------------	---

## bsc poll-timeout

To specify the timeout, in tenths of a second, for a poll or select sequence, use the **bsc poll-timeout** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc poll-timeout** *time*

**no bsc poll-timeout** *time*

<b>Syntax Description</b>	<i>time</i>	Time in tenths of a second. The default value is 10 (that is, 10 tenths of a second, or 1 second).
---------------------------	-------------	--

## bsc primary

To specify that the router is acting as the primary end of the Bisync link connected to the serial interface, and that the attached remote devices are Bisync tributary stations, use the **bsc primary** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc primary**

**no bsc primary**

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

## bsc retries

To specify the number of retries performed before a device is considered to have failed, use the **bsc retries** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc retries** *retries*

**no bsc retries** *retries*

<b>Syntax Description</b>	<i>retries</i>	Number of retries before a device fails. The default is 5.
---------------------------	----------------	--

## bsc secondary

To specify that the router is acting as the secondary end of the Bisync link connected to the serial interface, and the attached remote device is a Bisync control station, use the **bsc secondary** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc secondary**

**no bsc secondary**

---

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

## bsc servlim

To specify the number of cycles of the active poll list that are performed between polls to control units in the inactive poll list, use the **bsc servlim** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc servlim** *servlim-count*

**no bsc servlim** *servlim-count*

---

**Syntax Description** *servlim-count* Number of cycles. The range is 1 to 50. The default is 3.

---

## bsc spec-poll

To set specific polls, rather than general polls, used on the host-to-router connection, use the **bsc spec-poll** interface configuration command. To cancel the specification, use the **no** form of this command.

**bsc spec-poll**

**no spec-poll**

---

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

## bstun group

To specify the BSTUN group to which the interface belongs, use the **bstun group** interface configuration command. To remove the interface from the BSTUN group, use the **no** form of this command.

**bstun group** *group-number*

**no bstun group** *group-number*

---

### Syntax Description

<i>group-number</i>	BSTUN group to which the interface belongs.
---------------------	---

---

## bstun keepalive-count

To define the number of times to attempt a peer connection before declaring the peer connection to be down, use the **bstun keepalive-count** global configuration command. To cancel the definition, use the **no** form of this command.

**bstun keepalive-count** *count*

**no bstun keepalive-count**

---

### Syntax Description

<i>count</i>	Number of connection attempts. The range is between 2 and 10 retries.
--------------	---

---

## bstun lisnsap

To configure a SAP on which to listen for incoming calls, use the **bstun lisnsap** global configuration command. To cancel the SAP on which to listen, use the **no** form of this command.

**bstun lisnsap** *sap-value*

**no bstun lisnsap**

---

### Syntax Description

<i>sap-value</i>	SAP on which to listen for incoming calls. The default is 04.
------------------	---

---

## bstun peer-name

To enable the BSTUN function, use the **bstun peer-name** global configuration command. To disable the function, use the **no** form of this command.

```
bstun peer-name ip-address
```

```
no bstun peer-name ip-address
```

<b>Syntax Description</b>	<i>ip-address</i>	Address by which this BSTUN peer is known to other BSTUN peers that are using the TCP transport.
---------------------------	-------------------	--

## bstun protocol-group

To define a BSTUN group and the protocol it uses, use the **bstun protocol-group** global configuration command. To delete the BSTUN group, use the **no** form of this command.

```
bstun protocol-group group-number protocol
```

```
no bstun protocol-group group-number protocol
```

<b>Syntax Description</b>	<i>group-number</i>	BSTUN group number. Valid numbers are decimal integers in the range 1 to 255.
	<i>protocol</i>	Block serial protocol, selected from the following: <ul style="list-style-type: none"> <li>• <b>adplex</b></li> <li>• <b>adt-poll-select</b></li> <li>• <b>adt-vari-poll</b></li> <li>• <b>async-generic</b></li> <li>• <b>bsc</b></li> <li>• <b>bsc-local-ack</b></li> <li>• <b>diebold</b></li> <li>• <b>mdi</b></li> </ul>

## bstun remote-peer-keepalive

To enable detection of the loss of a peer, use the **bstun remote-peer-keepalive** global configuration command. To disable detection, use the **no** form of this command.

**bstun remote-peer-keepalive** *seconds*

**no bstun remote-peer-keepalive**

<b>Syntax Description</b>	<i>seconds</i>	Keepalive interval, in seconds. The range is 1 to 300 seconds. The default is 30 seconds.
---------------------------	----------------	---

## bstun route

To define how frames will be forwarded from a BSTUN interface to a remote BSTUN peer, use the **bstun route** interface configuration command. To cancel the definition, use the **no** form of this command.

**bstun route** {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*} [**direct**]

**no bstun route** {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*} [**direct**]

<b>Syntax Description</b>	<b>all</b>	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
	<b>address</b>	Serial frame that contains a specific address is propagated.
	<i>address-number</i>	Poll address, a hexadecimal number from 01 to FF (but not all values are valid). The reply address to be used on the return leg is calculated from the configured poll address.
	<b>tcp</b>	TCP encapsulation is used to propagate frames that match the entry.
	<i>ip-address</i>	IP address of the remote BSTUN peer.
	<b>interface serial</b>	HDLC encapsulation is used to propagate the serial frames.
	<i>number</i>	Serial line to an appropriately configured router on the other end.
	<b>direct</b>	(Optional) Specified interface is also a direct BSTUN link, rather than a serial connection to another peer.

## bstun route (Frame Relay)

To define how frames will be forwarded from a BSTUN interface to a remote BSTUN peer over Frame Relay, use the **bstun route** (Frame Relay) interface configuration command. To cancel the definition, use the **no** form of this command.

**bstun route** {**all** | **address** *cu-address*} **interface serial** *number* [**dldci** *dldci rsap*] [**priority** *priority*]

**no bstun route** {**all** | **address** *cu-address*} **interface serial** *number* [**dldci** *dldci rsap*] [**priority** *priority*]

<b>Syntax Description</b>	<b>all</b>	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
	<b>address</b>	Serial frames that contain a specific address are propagated.
	<i>cu-address</i>	Control unit address for the Bisync end station.
	<b>interface serial</b> <i>number</i>	Specify a serial interface on which Frame Relay encapsulation is used to propagate serial frames.
	<b>dlsi</b> <i>dlsi</i>	(Optional) Data-link connection identifier to be used on the Frame Relay interface.
	<i>rsap</i>	(Optional) Remote SAP, to be used when initiating an LLC2 session. This argument is configurable only if the interface group number supports local acknowledgment.
	<b>priority</b> <i>priority</i>	(Optional) Priority port to be used for this LLC2 session. Configurable only if the interface group number supports local acknowledgment.

## encapsulation bstun

To configure BSTUN on a particular serial interface, use the **encapsulation bstun** interface configuration command. To disable the BSTUN function on the interface, use the **no** form of this command.

**encapsulation bstun**

**no encapsulation bstun**

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

## encapsulation stun

To enable STUN encapsulation on a specified serial interface, use the **encapsulation stun** interface configuration command.

**encapsulation stun**

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

## frame-relay map bstun

To configure BSTUN over Frame Relay for passthrough, use the **frame-relay map bstun** interface configuration command. To cancel the configuration, use the **no** form of this command.

```
frame-relay map bstun dcli
```

```
no frame-relay map bstun dcli
```

Syntax Description	<i>dcli</i>	Frame Relay DLCI number on which to support passthrough.
--------------------	-------------	--

## priority-list protocol bstun

To establish BSTUN queueing priorities based on the BSTUN header, use the **priority-list protocol bstun** global configuration command. To revert to normal priorities, use the **no** form of this command.

```
priority-list list-number protocol bstun queue [gt | lt packet-size] [address bstun-group bsc-addr]
```

```
no priority-list list-number protocol bstun queue [gt | lt packet-size] [address bstun-group bsc-addr]
```

Syntax Description	<i>list-number</i>	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
	<i>queue</i>	Priority queue type: <b>high</b> , <b>medium</b> , <b>normal</b> , or <b>low</b> .
	<b>gt</b>   <b>lt</b> <i>packet-size</i>	(Optional) Output interface examines header information <i>and</i> packet size and places packets with the BSTUN header that match criteria ( <b>gt</b> or <b>lt</b> specified packet size) on specified output.
	<b>address</b> <i>bstun-group bsc-addr</i>	(Optional) Output interface examines header information and Bisync address and places packets with the BSTUN header that match Bisync address on the specified output queue.

## priority-list protocol ip tcp

To establish BSTUN or STUN queueing priorities based on the TCP port, use the **priority-list protocol ip tcp** global configuration command. To revert to normal priorities, use the **no** form of this command.

```
priority-list list-number protocol ip queue tcp tcp-port-number
```

```
no priority-list list-number protocol ip queue tcp tcp-port-number
```

Syntax Description	<i>list-number</i>	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
--------------------	--------------------	--

<i>queue</i>	Priority queue type: <b>high</b> , <b>medium</b> , <b>normal</b> , or <b>low</b> . The default <i>queue</i> value is <b>normal</b> .
<i>tcp-port-number</i>	<p>BSTUN port and priority settings are as follows:</p> <ul style="list-style-type: none"> <li>• High—BSTUN port 1976</li> <li>• Medium—BSTUN port 1977</li> <li>• Normal—BSTUN port 1978</li> <li>• Low—BSTUN port 1979</li> </ul> <p>STUN port and priority settings are as follows:</p> <ul style="list-style-type: none"> <li>• High—STUN port 1994</li> <li>• Medium—STUN port 1990</li> <li>• Normal—STUN port 1991</li> <li>• Low—STUN port 1992</li> </ul>

## priority-list protocol stun address

To establish STUN queueing priorities based on the address of the serial link, use the **priority-list protocol stun address** global configuration command. To revert to normal priorities, use the **no** form of this command.

**priority-list** *list-number* **protocol stun** *queue* **address** *group-number* *address-number*

**no** **priority-list** *list-number* **protocol stun** *queue-keyword* **address** *group-number* *address-number*

### Syntax Description

<i>list-number</i>	Arbitrary integer between 1 and 16 that identifies the priority list selected by the user.
<i>queue</i>	<p>Enables a priority queue type: Valid queue values and their equivalent priority queue type level are:</p> <ul style="list-style-type: none"> <li>• <b>high</b>—Priority queue type is high.</li> <li>• <b>medium</b>—Priority queue type is medium.</li> <li>• <b>normal</b>—Priority queue type is normal.</li> <li>• <b>low</b>—Priority queue type is low.</li> </ul> <p>The default <i>queue</i> value is <b>normal</b>.</p>
<i>group-number</i>	Group number that is used in the <b>stun group</b> command.
<i>address-number</i>	Address of the serial link. For an SDLC link, the format is a 1-byte hexadecimal value (for example, C1). For a non-SDLC link, the address format can be specified by the <b>stun schema</b> command.

## queue-list protocol bstun

To customize BSTUN queueing priorities based on the BSTUN header, use the **queue-list protocol bstun** global configuration command. To revert to normal priorities, use the **no** form of this command.

```
queue-list list-number protocol bstun queue [gt | lt packet-size] [address bstun-group bsc-addr]
```

```
no queue-list list-number protocol bstun queue [gt | lt packet-size] [address bstun-group bsc-addr]
```

Syntax Description		
<i>list-number</i>		Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
<i>queue</i>		Enables a priority queue type: Valid queue-keyword values and their equivalent priority queue type level are: <ul style="list-style-type: none"> <li>• <b>high</b>—Priority queue type is high.</li> <li>• <b>medium</b>—Priority queue type is medium.</li> <li>• <b>normal</b>—Priority queue type is normal.</li> <li>• <b>low</b>—Priority queue type is low.</li> </ul>
<b>gt</b>   <b>lt</b> <i>packet-size</i>		(Optional) Output interface examines header information <i>and</i> packet size and places packets with the BSTUN header that match criteria ( <b>gt</b> or <b>lt</b> specified packet size) on specified output.
<b>address</b> <i>bstun-group bsc-addr</i>		(Optional) Output interface examines header information and Bisync address and places packets with the BSTUN header that match Bisync address on the specified output queue.

## queue-list protocol ip tcp

To customize BSTUN queueing priorities based on the TCP port, use the **queue-list protocol ip tcp** global configuration command. To revert to normal priorities, use the **no** form of this command.

```
queue-list list-number protocol ip queue tcp tcp-port-number
```

```
no queue-list list-number protocol ip queue tcp tcp-port-number
```

Syntax Description		
<i>list-number</i>		Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
<i>queue</i>		Enables a priority queue type: Valid queue-keyword values and their equivalent priority queue type level are: <ul style="list-style-type: none"> <li>• <b>high</b>—Priority queue type is high.</li> <li>• <b>medium</b>—Priority queue type is medium.</li> <li>• <b>normal</b>—Priority queue type is normal.</li> <li>• <b>low</b>—Priority queue type is low.</li> </ul> The default <i>queue</i> value is <b>normal</b> .

---

<i>tcp-port-number</i>	<p>BSTUN port and priority settings are as follows:</p> <ul style="list-style-type: none"> <li>• High—BSTUN port 1976</li> <li>• Medium—BSTUN port 1977</li> <li>• Normal—BSTUN port 1978</li> <li>• Low—BSTUN port 1979</li> </ul> <p>STUN port and priority settings are as follows:</p> <ul style="list-style-type: none"> <li>• High—STUN port 1994</li> <li>• Medium—STUN port 1990</li> <li>• Normal—STUN port 1991</li> <li>• Low—STUN port 1992</li> </ul>
------------------------	--

---

## sdhc virtual-multidrop

To allow SDLC broadcast address FF to be replicated for each of the STUN peers, so each of the end stations receive the broadcast frame, use the **sdhc virtual-multidrop** interface configuration command. To disable the SDLC broadcast feature, use the **no** form of this command.

**sdhc virtual-multidrop**

**no sdhc virtual-multidrop**

---

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

## show bsc

To display statistics about the interfaces on which Bisync is configured, use the **show bsc** privileged EXEC command.

**show bsc** [**group** *bstun-group-number*] [**address** *address-list*]

---

<b>Syntax Description</b>	<b>group</b> <i>bstun-group-number</i>	(Optional) BSTUN group number. Valid numbers are decimal integers in the range 1 to 255.
	<b>address</b> <i>address-list</i>	(Optional) List of poll addresses.

---

## show bstun

To display the current status of STUN connections, use the **show bstun** privileged EXEC command.

**show bstun** [**group** *bstun-group-number*] [**address** *address-list*]

<b>Syntax Description</b>	<b>group</b> <i>bstun-group-number</i>	(Optional) BSTUN group number. Valid numbers are decimal integers in the range 1 to 255.
	<b>address</b> <i>address-list</i>	(Optional) List of poll addresses.

## show stun

To display the current status of STUN connections, use the **show stun** privileged EXEC command.

```
show stun
```

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

## stun group

To place each STUN-enabled interface on a router in a previously defined STUN group, use the **stun group** interface configuration command. To remove an interface from a group, use the **no** form of this command.

```
stun group group-number
```

```
no stun group group-number
```

<b>Syntax Description</b>	<i>group-number</i>	Integer in the range 1 to 255.
---------------------------	---------------------	--------------------------------

## stun keepalive-count

To define the number of times to attempt a peer connection before declaring the peer connection to be down, use the **stun keepalive-count** global configuration command. To cancel the definition, use the **no** form of this command.

```
stun keepalive-count count
```

```
no stun keepalive-count
```

<b>Syntax Description</b>	<i>count</i>	Number of connection attempts. The range is between 2 and 10 retries.
---------------------------	--------------	---

## stun peer-name

To enable STUN for an IP address, use the **stun peer-name** global configuration command. To disable STUN for an IP address, use the **no** form of this command.

```
stun peer-name ip-address cls
```

```
no stun peer-name ip-address cls
```

Syntax Description		
	<i>ip-address</i>	IP address by which this STUN peer is known to other STUN peers.
	<b>cls</b>	Use Cisco Link Services (CLS) to access the Frame Relay network.

## stun protocol-group

To create a protocol group, use the **stun protocol-group** global configuration command. To remove an interface from the group, use the **no** form of this command.

```
stun protocol-group group-number { basic | sdlc [sdlc-tg] | schema }
```

```
no stun protocol-group
```

Syntax Description		
	<i>group-number</i>	Integer in the range 1 to 255.
	<b>basic</b>	Indicates a non-SDLC protocol.
	<b>sdlc</b>	Indicates an SDLC protocol.
	<b>sdlc-tg</b>	(Optional) Identifies the group as part of an SNA TG.
	<b>schema</b>	Indicates a custom protocol.

## stun quick-response

To enable STUN quick-response, which can be used with local acknowledgment, use the **stun quick-response** global configuration command. To disable STUN quick-response, use the **no** form of this command.

```
stun quick-response
```

```
no stun quick-response
```

Syntax Description	
	This command has no arguments or keywords.

## stun remote-peer-keepalive

To enable detection of the loss of a peer, use the **stun remote-peer-keepalive** global configuration command. To disable detection, use the **no** form of this command.

**stun remote-peer-keepalive** *seconds*

**no stun remote-peer-keepalive**

Syntax Description	<i>seconds</i>	Keepalive interval, in seconds. The range is 1 to 300 seconds. The default is 30 seconds.
--------------------	----------------	---

## stun route address interface dlci

To configure direct Frame Relay encapsulation between STUN peers with SDLC local acknowledgment, use the **stun route address interface dlci** interface configuration command. To disable the configuration, use the **no** form of this command.

**stun route address** *sdhc-addr* **interface** *frame-relay-port* **dlci** *number* *localsap* **local-ack** **cls**

**no stun route address** *sdhc-addr* **interface** *frame-relay-port* **dlci** *number* *localsap* **local-ack** **cls**

Syntax Description	<i>sdhc-addr</i>	Address of the serial interface.
	<i>frame-relay-port</i>	Port number.
	<i>number</i>	Data-link connection identifier (DLCI) number.
	<i>localsap</i>	Local connecting SAP.
	<b>local-ack</b>	Enable local acknowledgment.
	<b>cls</b>	Use Cisco Link Services (CLS) to access the Frame Relay network.

## stun route address interface serial

To forward all HDLC traffic on a serial interface, use the **stun route address interface serial** interface configuration command. To disable this method of HDLC encapsulation, use the **no** form of this command.

**stun route address** *address-number* **interface** **serial** *number* [**direct**]

**no stun route address** *address-number* **interface** **serial** *number*

Syntax Description	<i>address-number</i>	Address of the serial interface.
	<i>number</i>	Number assigned to the serial interface.
	<b>direct</b>	(Optional) Forwards all HDLC traffic on a direct STUN link.

## stun route address tcp

To specify TCP encapsulation and optionally establish SDLC local acknowledgment (SDLC transport) for STUN, use the **stun route address tcp** interface configuration command. To disable this method of TCP encapsulation, use the **no** form of this command.

```
stun route address address-number tcp ip-address [local-ack] [priority] [tcp-queue-max]
[passive]
```

```
no stun route address address-number tcp ip-address [local-ack] [priority] [tcp-queue-max]
[passive]
```

### Syntax Description

<i>address-number</i>	Number that conforms to SDLC addressing conventions.
<i>ip-address</i>	IP address by which this STUN peer is known to other STUN peers that are using the TCP as the STUN encapsulation.
<b>local-ack</b>	(Optional) Enables local acknowledgment for STUN.
<b>priority</b>	(Optional) Establishes the four levels used in priority queuing: low, medium, normal, and high.
<b>tcp-queue-max</b>	(Optional) Sets the maximum size of the outbound TCP queue for the SDLC link. The default is 100.
<b>passive</b>	(Optional) Prevents the STUN peer from initiating a TCP connection. Normally, the STUN peer connects to the SDLC primary device and initiates a TCP connection to another STUN peer. If the STUN peers connect to non-SDLC devices, such as voice equipment, both STUN peers might try to start a TCP connection at the same time, which can delay the TCP connection setup.  The <b>passive</b> keyword, used in STUN basic mode, enables this STUN peer to wait for the other STUN peer to initiate the TCP connection.

## stun route all interface serial

To encapsulate and forward all STUN traffic using HDLC encapsulation on a serial interface, use the **stun route all interface serial** interface configuration command. To disable this method of encapsulation, use the **no** form of this command.

```
stun route all interface serial number [direct]
```

```
no stun route all interface serial number [direct]
```

### Syntax Description

<i>number</i>	Number assigned to the serial interface.
<b>direct</b>	(Optional) Indicates that the specified interface is also a direct STUN link, rather than a serial connection to another peer.

## stun route all tcp

To forward all STUN traffic on an interface regardless of which address is contained in the serial frame, use the **stun route all tcp** interface configuration command with TCP encapsulation. To disable traffic from being forwarded with this method of encapsulation, use the **no** form of this command.

**stun route all tcp** *ip-address* [**passive**]

**no stun route all tcp** *ip-address* [**passive**]

Syntax Description		
	<i>ip-address</i>	IP address by which this remote STUN peer is known to other STUN peers. Use the address that identifies the remote STUN peer that is connected to the remote serial link.
	<b>passive</b>	(Optional) Prevents the STUN peer from initiating a TCP connection. Normally, the STUN peer connects to the SDLC primary device and initiates a TCP connection to another STUN peer. If the STUN peers connect to non-SDLC devices, such as voice equipment, both STUN peers might start a TCP connection at the same time. The <b>passive</b> keyword enables a delay when setting up a TCP connection.

## stun schema offset length format

To define a protocol other than SDLC for use with STUN, use the **stun schema offset length format** global configuration command. To disable the new protocol, use the **no** form of this command.

**stun schema** *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

**no stun schema** *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

Syntax Description		
	<i>name</i>	Name that defines your protocol. It can be up to 20 characters in length.
	<i>constant-offset</i>	Constant offset, in bytes, for the address to be found in the frame.
	<i>address-length</i>	Length in one of the following formats: decimal (4 bytes), hexadecimal (8 bytes), or octal (4 bytes).
	<i>format-keyword</i>	Identifies format to be used to specify and display addresses for routes on interfaces that use this STUN protocol. Valid format keyword values and their ranges are: <ul style="list-style-type: none"> <li>• <b>decimal</b>—0 to 9</li> <li>• <b>hexadecimal</b>—0 to F</li> <li>• <b>octal</b>—0 to 7</li> </ul>

## stun sdlc-role primary

To assign the router the role of SDLC primary node, use the **stun sdlc-role primary** interface configuration command. Primary nodes poll secondary nodes in a predetermined order. To disable the primary node role assignment, use the **no** form of this command.

**stun sdlc-role primary**

**no stun sdlc-role**

---

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

## stun sdlc-role secondary

To assign the router the role of SDLC secondary node, use the **stun sdlc-role secondary** interface configuration command. Secondary nodes respond to polls sent by the SDLC primary by transmitting any outgoing data they may have. To disable the assignment, use the **no** form of this command.

**stun sdlc-role secondary**

**no stun sdlc-role**

---

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

■ `stun sdlc-role secondary`



## LLC2 and SDLC Commands

---

This chapter describes the function and syntax of the Logical Link Control, type 2 (LLC2) and SDLC commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### encapsulation sdlc

To configure an SDLC interface, use the **encapsulation sdlc** interface configuration command. To deactivate the command, use the **no** form of this command.

**encapsulation sdlc**

**no encapsulation sdlc**

---

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

### encapsulation sdlc-primary

To configure the router as the primary SDLC station if you plan to configure the SDLLC media translation feature, use the **encapsulation sdlc-primary** interface configuration command. To deactivate the command, use the **no** form of this command.

**encapsulation sdlc-primary**

**no encapsulation sdlc-primary**

---

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

## encapsulation sdlc-secondary

To configure the router as a secondary SDLC station if you plan to configure the SDLLC media translation feature, use the **encapsulation sdlc-secondary** interface configuration command. To deactivate the command, use the **no** form of this command.

**encapsulation sdlc-secondary**

**no encapsulation sdlc-secondary**

---

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

## llc2 ack-delay-time

To set the amount of time the Cisco IOS software waits for an acknowledgment before sending the next set of information frames, use the **llc2 ack-delay-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 ack-delay-time** *milliseconds*

**no llc2 ack-delay-time** *milliseconds*

---

<b>Syntax Description</b>	<i>milliseconds</i>	Number of milliseconds the software allows incoming information frames to stay unacknowledged. The minimum is 1 ms and the maximum is 60000 ms. The default is 100 ms.
---------------------------	---------------------	--

---

## llc2 ack-max

To control the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment, use the **llc2 ack-max** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 ack-max** *packet-count*

**no llc2 ack-max** *packet-count*

---

<b>Syntax Description</b>	<i>packet-count</i>	Maximum number of packets the software will receive before sending an acknowledgment. The minimum is 1 packet and the maximum is 127 packets. The default is 3 packets.
---------------------------	---------------------	---

---

## llc2 idle-time

To control the frequency of polls during periods of idle time (no traffic), use the **llc2 idle-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 idle-time** *milliseconds*

**no llc2 idle-time** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of ms that can pass with no traffic before the LLC2 station sends a Receiver Ready frame. The minimum is 1 ms and the maximum is 60000 ms. The default is 10000 ms.
---------------------------	---------------------	--

## llc2 local-window

To control the maximum number of information frames the Cisco IOS software sends before it waits for an acknowledgment, use the **llc2 local-window** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 local-window** *packet-count*

**no llc2 local-window** *packet-count*

<b>Syntax Description</b>	<i>packet-count</i>	Maximum number of packets that can be sent before the software must wait for an acknowledgment. The minimum is 1 packet and the maximum is 127 packets. The default is 7 packets.
---------------------------	---------------------	---

## llc2 n1

To specify the maximum size of an I-frame, use the **llc2 n1** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 n1** *bytes*

**no llc2 n1**

<b>Syntax Description</b>	<i>bytes</i>	Maximum size of an I-frame. The valid range is 1 to 4105 bytes. The default is 4105 bytes.
---------------------------	--------------	--

## llc2 n2

To control the amount of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations, use the **llc2 n2** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 n2** *retry-count*

**no llc2 n2**

<b>Syntax Description</b>	<i>retry-count</i>	Number of times the software retries operations. The minimum is 1 retry and the maximum is 255 retries. The default is 8 retries.
---------------------------	--------------------	---

## llc2 nw

To increase the window size for consecutive good I-frames received, use the **llc2 nw** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 nw** *window-size-increase*

**no llc2 nw**

<b>Syntax Description</b>	<i>window-size-increase</i>	Number of frames to increase the window size for consecutive good I-frames received (0 is disabled). The default is 0.
---------------------------	-----------------------------	--

## llc2 recv-window

To control the number of frames in the receive window, use the **llc2 recv-window** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 recv-window** *frame-count*

**no llc2 recv-window**

<b>Syntax Description</b>	<i>frame-count</i>	Specifies the number of frames in the receive window. The default is 7.
---------------------------	--------------------	---

## llc2 send-window

To control the number of frames in the send window, use the **llc2 send-window** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 send-window** *frame-count*

**no llc2 send-window**

<b>Syntax Description</b>	<i>frame-count</i>	Specifies the number of frames in the send window. The default is 7.
---------------------------	--------------------	--

## llc2 t1-time

To control the amount of time the Cisco IOS software will wait before resending unacknowledged information frames, use the **llc2 t1-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 t1-time** *milliseconds*

**no llc2 t1-time** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of milliseconds the software waits before resending unacknowledged information frames. The minimum is 1 ms and the maximum is 60000 ms. The default is 1000 ms.
---------------------------	---------------------	--

## llc2 tbusy-time

To control the amount of time the Cisco IOS software waits until repolling a busy remote station, use the **llc2 tbusy-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 tbusy-time** *milliseconds*

**no llc2 tbusy-time** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of ms the software waits before repolling a busy remote station. The minimum is 1 ms and the maximum is 60000 ms. The default is 9600 ms.
---------------------------	---------------------	--

## llc2 tpf-time

To set the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame, use the **llc2 tpf-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 tpf-time** *milliseconds*

**no llc2 tpf-time** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of ms the software waits for a final response to a poll frame before resending the poll frame. The minimum is 1 ms and the maximum is 60000 ms. The default is 1000 ms.
---------------------------	---------------------	--

## llc2 trej-time

To control the amount of time the Cisco IOS software waits for a correct frame after sending a reject command to the remote LLC2 station, use the **llc2 trej-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 trej-time** *milliseconds*

**no llc2 trej-time** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of milliseconds the software waits for a resend of a rejected frame before sending a reject command to the remote station. The minimum is 1 ms and the maximum is 60000 ms. The default is 3200 ms.
---------------------------	---------------------	--

## llc2 xid-neg-val-time

To control the frequency of exchange of identification (XID) transmissions by the Cisco IOS software, use the **llc2 xid-neg-val-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 xid-neg-val-time** *milliseconds*

**no llc2 xid-neg-val-time** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of ms after which the software sends XID frames to other LLC2-speaking stations. The minimum is 0 ms and the maximum is 60000 ms. The default is 0 ms.
---------------------------	---------------------	---

## llc2 xid-retry-time

To set the amount of time the Cisco IOS software waits for a reply to exchange of identification (XID) frames before dropping the session, use the **llc2 xid-retry-time** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

**llc2 xid-retry-time** *milliseconds*

**no llc2 xid-retry-time** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of ms the software waits for a reply to XID frames before dropping a session. The minimum is 1 ms and the maximum is 60000 ms. The default is 60000 ms.
---------------------------	---------------------	--

## sdlc address

To assign a set of secondary stations attached to the serial link, use the **sdlc address** interface configuration command. To remove an assigned secondary station use the **no** form of this command.

To assign the IBM reserved address ff as a non-broadcast valid local address, configure the **sdlc address** interface configuration command with a hexbyte value of *ff* and specify the **ack-mode** option. To deactivate, use the **no** form of this command.

**sdlc address** *hexbyte* [**echo**] [**ack-mode**] [**xid-poll**] [**switched**] [**seonly**] [**xid-passthru**] [**passive**] [**K number**]

**no sdlc address** *hexbyte* [**echo**] [**ack-mode**] [**xid-poll**] [**switched**] [**seonly**] [**xid-passthru**] [**passive**] [**K number**]

<b>Syntax Description</b>	<i>hexbyte</i>	Hexadecimal number (base 16) that indicates the address of the serial link. The range is 1 to ff. If ff is configured, the <b>ack-mode</b> option must be specified.
<b>echo</b>		(Optional) Treats non-echo and echo SDLC addresses as the same address.
<b>ack-mode</b>		(Optional) Supports applications that require local termination of an SDLC connection with address FF. This option should be used only if you use the SDLC address ff as a regular (not a broadcast) address.
<b>xid-poll</b>		(Optional) Configures the router to send a null XID to the Token Ring-attached host device. This tells the host device to start the session.
<b>switched</b>		(Optional) Configures the router to send an exchange identification (XID) to an SDLC attached device. When the device answers, then a proxy XID is sent to the peer.
<b>seonly</b>		(Optional) Eliminates the need for counting PU4 lines on the Network Control Program (NCP) to determine the correct poll address. Since the router is always secondary, when <b>seonly</b> is coded, the polling address will be determined by the router.
<b>xid-passthru</b>		(Optional) Allows the router to pass the (XID) through the interface in both the host and end device's direction.

<b>passive</b>	(Optional) Causes the router to wait before sending a SNRM until it receives an XID from the host. This keyword is valid only when the role is primary, and it requires the <b>sdhc partner</b> command with keyword <b>inbound</b> specified.
<b>K number</b>	(Optional) Specifies the maximum number of information frames (I-frames) that a router can send before it expects an acknowledgment from the end device. The minimum window-size is 1 and the maximum size is 7. The default is 7.

## sdhc dte-timeout

To adjust the amount of time a data terminal equipment (DTE) interface waits for the data circuit-terminating equipment (DCE) to assert a Clear To Send (CTS) signal before dropping a Request To Send (RTS), use the **sdhc dte-timeout** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdhc dte-timeout** *unit*

**no sdhc dte-timeout** *unit*

<b>Syntax Description</b>	<i>unit</i>	Timeout wait interval in microseconds. The valid range is 10 to 64000. Each unit is approximately 5 microseconds. The default is 10 units (approximately 50 microseconds).
---------------------------	-------------	--

## sdhc frmr-disable

To indicate that secondary stations on a particular serial link do not support Frame Rejects (FRMRs) or error indications, use the **sdhc frmr-disable** interface configuration command. To specify that the secondary station does support FRMRs, use the **no** form of this command.

**sdhc frmr-disable**

**no sdhc frmr-disable**

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

## sdhc holdq

To control the maximum number of packets that can be held in a buffer before being sent to a remote SDLC station, use the **sdhc holdq** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdhc holdq** *address queue-size*

**no sdhc holdq** *address queue-size*

<b>Syntax Description</b>	<i>address</i>	SDLC address for which you are specifying a queue size.
	<i>queue-size</i>	Local send window size. The minimum is 1 packet. No maximum value has been established. The default is 200 packets.

## sdlc k

To set the window size in order to control the maximum number of information frames the Cisco IOS software sends before it must stop sending and wait for an acknowledgment from the receiving router, use the **sdlc k** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdlc k** *window-size*

**no sdlc k** *window-size*

<b>Syntax Description</b>	<i>window-size</i>	Local send window size. The minimum is 1 frame. The maximum is 7 frames, which is the default.
---------------------------	--------------------	--

## sdlc line-speed

To enable adaptive SDLC T1, use the **sdlc line-speed** interface configuration command. To deactivate the command, use the **no** form of this command.

**sdlc line-speed** *rate*

**no sdlc line-speed** *rate*

<b>Syntax Description</b>	<i>rate</i>	Clock rate in bits per second.
---------------------------	-------------	--------------------------------

## sdlc n1

To control the maximum size of an incoming frame, use the **sdlc n1** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdlc n1** *bit-count*

**no sdlc n1** *bit-count*

<b>Syntax Description</b>	<i>bit-count</i>	Number indicating bit size. Frames that exceed this size are rejected. The minimum is 1 bit. The maximum is 12000 bits, which is the default.
---------------------------	------------------	---

## sdlc n2

To determine the number of times that the Cisco IOS software resends a frame before terminating the SDLC session, use the **sdlc n2** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdlc n2** *retry-count*

**no sdlc n2** *retry-count*

<b>Syntax Description</b>	<i>retry-count</i>	Number of retry attempts. When this number is exceeded, the SDLC station terminates its session with the other station. The minimum is 1 and the maximum is 255. The default is 20 retries.
---------------------------	--------------------	---

## sdlc partner

To specify the destination address with which an LLC session is established for the SDLC station, use the **sdlc partner** interface configuration command. To cancel the configuration, use the **no** form of this command.

**sdlc partner** *mac-address sdlc-address* {**inbound** | **outbound**}

**no sdlc partner** *mac-address sdlc-address* {**inbound** | **outbound**}

<b>Syntax Description</b>	<i>mac-address</i>	The 48-bit Media Access Control (MAC) address of the Token Ring host.
	<i>sdlc-address</i>	SDLC address of the serial device that will communicate with the Token Ring host. The valid range is 1 to FE.
	<b>inbound</b>	Prevents the router from sending proxy XIDs to the remote end station on behalf of the station specified. The remote end station must initiate the connection. When the router is configured for SDLC role secondary, the default is inbound (the router does not send proxy XIDs until it is polled).  The <b>inbound</b> keyword is required if you want the router to wait before sending an SNRM until it receives an XID from the host. See the <b>passive</b> keyword on the <b>sdlc address</b> command for more details.
	<b>outbound</b>	Causes the router to send proxy XIDs to the partner end station. If the remote end station responds, then (for PU 2.1 local devices) a NULL XID is sent on the SDLC line. The default behavior for SDLC role primary is outbound, and for SDLC role secondary is inbound.

## sdhc poll-limit-value

To control how many times a single secondary station can be polled for input before the next station must be polled, use the **sdhc poll-limit-value** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdhc poll-limit-value** *count*

**no sdhc poll-limit-value** *count*

<b>Syntax Description</b>	<i>count</i>	Number of times the Cisco IOS software can poll one secondary station before proceeding to the next station. The valid range is 1 through 10. The default is 1.
---------------------------	--------------	---

## sdhc poll-pause-timer

To control how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface, use the **sdhc poll-pause-timer** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdhc poll-pause-timer** *milliseconds*

**no sdhc poll-pause-timer** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of ms that the software waits before sending the poll frame to a single serial interface. This is a number in the range 1 to 10000. The default is 10 ms.
---------------------------	---------------------	--

## sdhc poll-wait-timeout

To specify the interval the Cisco IOS software will wait for polls from a primary node before timing out that connection when the router has been configured for local acknowledgment and some form of SDLC communication (SDLLC or STUN, for example), use the **sdhc poll-wait-timeout** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdhc poll-wait-timeout** *milliseconds*

**no sdhc poll-wait-timeout** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Number of milliseconds the software will wait for a poll from the primary station before timing out the connection to the primary station. The minimum is 10 ms and the maximum is 64000 ms. The default is 10000 ms.
---------------------------	---------------------	---

## sdhc qlc-prtnr

To establish correspondence between an SDLC and QLLC connection, use the **sdhc qlc-prtnr** interface configuration command. To deactivate the command, use the **no** form of this command.

```
sdhc qlc-prtnr virtual-mac-address sdlc-address
```

```
no sdhc qlc-prtnr virtual-mac-address sdlc-address
```

### Syntax Description

<i>virtual-mac-address</i>	The virtual Media Access Control (MAC) address in the form <i>h.h.h</i> .
<i>sdlc-address</i>	SDLC address in hexadecimal. The valid range is 1 to FE.

## sdhc role

To establish the router to be either a primary or secondary SDLC station, use the **sdhc role** interface configuration command. To cancel the designation, use the **no** form of this command.

```
sdhc role { none | primary | secondary | prim-xid-poll }
```

```
no sdhc role { none | primary | secondary | prim-xid-poll }
```

### Syntax Description

<b>none</b>	Establishes the router as either a primary or secondary station, depending on the end stations.
<b>primary</b>	Establishes the router as a primary station.
<b>secondary</b>	Establishes the router as a secondary station.
<b>prim-xid-poll</b>	Establishes the router as a primary station when the end station is configured as a secondary NT2.1.

## sdhc saps

To configure SDLC-to-LLC sessions with respect to the SSAP and DSAP on the LLC, use the **sdhc saps** interface configuration command. To return to the default setting, use the **no** form of this command.

```
sdhc saps address ssap dsap
```

```
no sdhc saps address ssap dsap
```

### Syntax Description

<i>address</i>	Address of the SDLC station that will communicate with the router. Valid range is 1 to FF.
<i>ssap</i>	Source service access point (SSAP) of the partner. Valid range is 1 to FF.
<i>dsap</i>	Destination service access point (DSAP) of the partner. Valid range is 1 to FF.

## sdlc sdlc-largest-frame

To indicate the largest information frame (I-frame) size that can be sent or received by the designated SDLC station, use the **sdlc sdlc-largest-frame** interface configuration command. To return to the default value, use the **no** form of this command.

**sdlc sdlc-largest-frame** *address size*

**no sdlc sdlc-largest-frame** *address size*

Syntax Description		
	<i>address</i>	Address of the SDLC station that will communicate with the router.
	<i>size</i>	Largest frame size that can be sent or received. The default is 265 bytes.

## sdlc simultaneous

To enable an interface configured as a primary SDLC station to operate in two-way simultaneous mode, use the **sdlc simultaneous** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdlc simultaneous** [**full-datamode** | **half-datamode**]

**no sdlc simultaneous** [**full-datamode** | **half-datamode**]

Syntax Description		
	<b>full-datamode</b>	(Optional) Enables the primary station to send data to and receive data from the polled secondary station.
	<b>half-datamode</b>	(Optional) Prohibits the primary station from sending data to the polled secondary station.

## sdlc slow-poll

To enable the slow-poll capability of the router as a primary SDLC station, use the **sdlc slow-poll** interface configuration command. To disable slow-poll capability, use the **no** form of this command.

**sdlc slow-poll** *seconds*

**no sdlc slow-poll**

Syntax Description		
	<i>seconds</i>	Amount of time in seconds. The default is 10 seconds.

## sdhc snrm-timer

To specify a SNRM timer that is different from the T1 response time, set the SDLC SNRM timer using the **sdhc snrm-timer** command in interface configuration mode. To deactivate, use the **no** form of this command.

**sdhc snrm-timer** *number*

**no sdhc snrm-timer** *number*

### Syntax Description

<i>number</i>	Specifies the time to wait for a reply to a SNRM frame in milliseconds, and is enabled only if the station role is primary. Range is 1 to 64000 ms, and default is the <b>no</b> form of the command.
---------------	---

## sdhc t1

To control the amount of time the Cisco IOS software waits for an acknowledgment to a frame or sequence of frames, use the **sdhc t1** interface configuration command. To revert to the default setting, use the **no** form of this command.

**sdhc t1** *milliseconds*

**no sdhc t1** *milliseconds*

### Syntax Description

<i>milliseconds</i>	Number of milliseconds that the software waits. The minimum is 1 ms and the maximum is 64000 ms. The default is 3000 ms.
---------------------	--

## sdhc test serial

To determine the status of end stations, use the **sdhc test serial EXEC** command. To halt the sending of the test frames, use the **sdhc test serial** command with the **stop** keyword.

**sdhc test serial** *number address [iterations | continuous | stop | string string]*

### Syntax Description

<i>number</i>	Serial interface on which the test frame is to be sent out.
<i>address</i>	SDLC address (in hexadecimal) of the end station to receive the test frame.
<i>iterations</i>	(Optional) Number of test frames to be sent. The valid range is 1 to 25 frames. The default is 10 frames.
<b>continuous</b>	(Optional) Sends frames continuously until the <b>sdhc test serial</b> command is issued with the <b>stop</b> keyword.
<b>stop</b>	(Optional) Halts the sending of test frames.
<b>string</b> <i>string</i>	(Optional) Specifies a string of characters as data within the test frame. If this option is not specified, the default test string is ABCDEFGHIJKLMNOPQRSTUVWXYZ.

## sdlc vmac

To configure a MAC address for the serial interface, use the **sdlc vmac** interface configuration command. To disable the configuration, use the **no** form of this command.

**sdlc vmac** *mac-address*

**no sdlc vmac** *mac-address*

<b>Syntax Description</b>	<i>mac-address</i>	48-bit MAC address of the Token Ring host.
---------------------------	--------------------	--

## sdlc xid

To specify an XID value appropriate for the designated SDLC station associated with this serial interface, use the **sdlc xid** interface configuration command. To disable XID processing for this address, use the **no** form of this command.

**sdlc xid** *address xid*

**no sdlc xid** *address xid*

<b>Syntax Description</b>	<i>address</i>	Address of the SDLC station associated with this interface.
	<i>xid</i>	XID the Cisco IOS software will use to respond to XID requests the router receives. This value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

## sdlc xid-pause-timer

To control the frequency of XID retries between a router and an upstream VTAM, use the **sdlc xid-pause-timer** interface configuration command. To restore the default timer value, use the **no** form of this command.

**sdlc xid-pause-timer** *time*

**no sdlc xid-pause-timer** *time*

<b>Syntax Description</b>	<i>time</i>	Length of time the router is to wait, in seconds, before sending the next retry XID. The valid range is 10 to 300 seconds. The default is 10 seconds.
---------------------------	-------------	---

# show llc2

To display the LLC2 connections active in the router, use the **show llc2** privileged EXEC command.

```
show llc2
```

---

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



## IBM Network Media Translation Commands

---

This chapter describes the function and syntax of the IBM network media translation commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### qlc accept-all-calls

To enable the router to accept a call from any remote X.25 device, use the **qlc accept-all-calls** interface configuration command. To cancel the request, use the **no** form of this command.

**qlc accept-all-calls**

**no qlc accept-all-calls**

---

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

### qlc largest-packet

To indicate the maximum size of the Systems Network Architecture (SNA) packet that can be sent or received on an X.25 interface configured for QLLC conversion, use the **qlc largest-packet** interface configuration command. To restore the default largest packet size, use the **no** form of this command.

**qlc largest-packet** *virtual-mac-addr max-size*

**no qlc largest-packet** *virtual-mac-addr max-size*

---

<b>Syntax Description</b>	<i>virtual-mac-addr</i>	Virtual MAC address associated with the remote X.25 device, as defined using the <b>x25 map qlc</b> or <b>x25 pvc qlc</b> interface configuration commands. This address is written as a dotted triple of four-digit hexadecimal numbers.
	<i>max-size</i>	Maximum size, in bytes, of the SNA packet that can be sent or received on the X.25 interface configured for QLLC conversion. This value agrees with the value configured in the remote SNA device. The valid range is 0 to 1024.

---

## qlc npsi-poll

To enable a connection between a PU 2 on the LAN side and a front-end processor (FEP) running NPSI on the X.25 side, use the **qlc npsi-poll** interface configuration command. To disable this capability, use the **no** form of this command.

**qlc npsi-poll** *virtual-mac-addr*

**no qlc npsi-poll** *virtual-mac-addr*

### Syntax Description

---

*virtual-mac-addr* MAC address associated with the remote X.25 device, as defined using the **x25 map qlc** or **x25 pvc qlc** interface configuration commands. This address is written as a dotted triple of four-digit hexadecimal numbers.

---

## qlc partner

To enable a router configured for QLLC conversion to open a connection to the local Token Ring device on behalf of the remote X.25 device when an incoming call is received, use the **qlc partner** interface configuration command. To disable this capability, use the **no** form of this command.

**qlc partner** *virtual-mac-addr mac-addr*

**no qlc partner** *virtual-mac-addr mac-addr*

### Syntax Description

---

<i>virtual-mac-addr</i>	MAC address associated with the remote X.25 device, as defined using the <b>x25 map qlc</b> or <b>x25 pvc qlc</b> interface configuration commands. This address is written as a dotted triple of four-digit hexadecimal numbers.
<i>mac-addr</i>	48-bit MAC address of the Token Ring host that will communicate with the remote X.25 device.

---

## qlc sap

To associate a service access point (SAP) value other than the default SAP value with a serial interface configured for X.25 communication and QLLC conversion, use the **qlc sap** interface configuration command. To return this SAP value to its default state, use the **no** form of this command.

**qlc sap** *virtual-mac-addr ssap dsap*

**no qlc sap** *virtual-mac-addr ssap dsap*

### Syntax Description

---

<i>virtual-mac-addr</i>	MAC address associated with the remote X.25 device, as defined using the <b>x25 map qlc</b> or <b>x25 pvc qlc</b> interface configuration commands. This address is written as a dotted triple of four-digit hexadecimal numbers.
-------------------------	---

---

<i>ssap</i>	Source SAP value. It can be a decimal number in the range 2 to 254. The default is 4.
<i>dsap</i>	Destination SAP value. It can be a decimal number in the range 2 to 254. The default is 4.

## qllc srb

To enable QLLC conversion on a serial interface configured for X.25 communication, use the **qllc srb** interface configuration command. To disable QLLC conversion on the interface, use the **no** form of this command.

**qllc srb** *virtual-mac-addr* *srn* *trn*

**no qllc srb** *srn* *trn*

### Syntax Description

<i>virtual-mac-addr</i>	MAC address associated with the remote X.25 device, as defined using the <b>x25 map qllc</b> or <b>x25 pvc qllc</b> interface configuration commands. It can be 1 to 15 digits long.
<i>srn</i>	Source ring number. This value defines a virtual ring for all of the remote X.25 devices attached to the QLLC interface.
<i>trn</i>	Target ring number. It must be a virtual ring group that has been defined with the <b>source-bridge sdllc-local-ack</b> global configuration command.

## qllc xid

To associate an exchange ID (XID) value with the remote X.25 device that communicates through the Cisco IOS software using QLLC conversion, use the **qllc xid** interface configuration command. To disable XID processing for this address, use the **no** form of this command.

**qllc xid** *virtual-mac-addr* *xid*

**no qllc xid** *virtual-mac-addr* *xid*

### Syntax Description

<i>virtual-mac-addr</i>	MAC address associated with the remote X.25 device, as defined using the <b>x25 map qllc</b> or <b>x25 pvc qllc</b> interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
<i>xid</i>	Combined XID IDBLK and XID IDNUM you are associating with the X.25 device at this X.121 address. This hexadecimal value must be four bytes (eight digits) in length.

## sdllc partner

To enable device-initiated connections for SDLLC, use the **sdllc partner** interface configuration command. This command must be specified for the serial interface that links to the serial line device. To cancel the original instruction, use the **no** form of this command.

**sdllc partner** *mac-address sdlc-address*

**no sdllc partner** *mac-address sdlc-address*

Syntax Description	mac-address	MAC address of the Token Ring host.
	sdlc-address	SDLC address of the serial device that will communicate with the Token Ring host.

## sdllc ring-largest-frame

To indicate the largest I-frame size that can be sent to or received from the LLC2 primary station, use the **sdllc ring-largest-frame** interface configuration command. To return to the default, use the **no** form of this command.

**sdllc ring-largest-frame** *value*

**no sdllc ring-largest-frame** *value*

Syntax Description	value	Frame size in bytes. Possible values include 516, 1500, 2052, 4472, 8144, 11407, and 17800. The default is 516 bytes.
--------------------	-------	---

## sdllc sap

To associate a SAP value other than the default SAP value with a serial interface configured for SDLLC, use the **sdllc sap** interface configuration command. To return this SAP value to its default state, use the **no** form of this command.

**sdllc sap** *sdlc-address ssap dsap*

**no sdllc sap** *sdlc-address ssap dsap*

Syntax Description	sdlc-address	MAC address associated with the remote SDLC device.
	ssap	Source SAP value. It must be in the range 1 to 254. The default is 4.
	dsap	Destination SAP value. It must be in the range 1 to 254. The default is 4.

## sdllc sdlc-largest-frame

To indicate the largest information frame (I-frame) size that can be sent or received by the designated SDLC station, use the **sdllc sdlc-largest-frame** interface configuration command. To return to the default value, use the **no** form of this command.

**sdllc sdlc-largest-frame** *address value*

**no sdllc sdlc-largest-frame** *address value*

Syntax Description		
	<i>address</i>	Address of the SDLC station that will communicate with the Token Ring host.
	<i>value</i>	Largest frame size that can be sent or received by this SDLC station. The default is 265 bytes.

## sdllc traddr

To enable SDLLC media translation on a serial interface, use the **sdllc traddr** interface configuration command. The address specified is a MAC address to be assigned to the serial station. To disable SDLLC media translation on the interface, use the **no** form of this command.

**sdllc traddr** *xxxx.xxxx.xx00 lr bn tr*

**no sdllc traddr** *xxxx.xxxx.xx00 lr bn tr*

Syntax Description		
	<i>xxxx.xxxx.xx00</i>	MAC address to be assigned to the serial interface.
	<i>lr</i>	SDLLC virtual ring number.
	<i>bn</i>	SDLLC bridge number.
	<i>tr</i>	SDLLC target ring number.

## sdllc xid

To specify an XID value appropriate for the designated SDLC station associated with this serial interface, use the **sdllc xid** interface configuration command. To disable XID processing for this address, use the **no** form of this command.

**sdllc xid** *address xxxxxxxx*

**no sdllc xid** *address xxxxxxxx*

Syntax Description		
	<i>address</i>	Address of the SDLC station associated with this interface.
	<i>xxxxxxxx</i>	XID the Cisco IOS software will use to respond to XID requests received on the Token Ring (LLC2) side of the connection. This value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

## show qlc

To display the current state of any QLLC connections, use the **show qlc** privileged EXEC command.

```
show qlc
```

---

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

## show sdllc local-ack

To display the current state of any current local acknowledgment connections, and any configured passthrough rings, use the **show sdllc local-ack** privileged EXEC command.

```
show sdllc local-ack
```

---

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

## source-bridge qlc-local-ack

To enable or disable QLLC local acknowledgment for all QLLC conversion connections, use the **source-bridge qlc-local-ack** global configuration command. To disable this capability, use the **no** form of this command.

```
source-bridge qlc-local-ack
```

```
no source-bridge qlc-local-ack
```

---

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

## source-bridge remote-peer interface

When specifying a point-to-point direct encapsulation connection, use the **source-bridge remote-peer interface** global configuration command. To disable previous interface assignments, use the **no** form of this command.

```
source-bridge remote-peer ring-group interface interface-name [mac-address] [if size]
```

```
no source-bridge remote-peer ring-group interface interface-name
```

<b>Syntax Description</b>	<i>ring-group</i>	Ring group number. This ring group number must match the number you have specified with the <b>source-bridge ring-group</b> command. The valid range is 1 to 4095.
	<i>interface-name</i>	Name of the serial interface over which to send source-route bridged traffic.
	<i>mac-address</i>	(Optional) MAC address for the interface you specify using the <i>interface-name</i> argument. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the <b>show interfaces</b> command, and then scanning the display for the interface specified by <i>interface-name</i> .
	<b>if size</b>	(Optional) Maximum size frame to be sent to this remote peer. The Cisco IOS software negotiates all transit routes down to this size or lower. This argument is useful in preventing timeouts in end hosts by reducing the amount of data they have to send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

## source-bridge sdllc-local-ack

To activate local acknowledgment for SDLLC sessions on a particular interface, use the **source-bridge sdllc-local-ack** global configuration command. To deactivate local acknowledgment for SDLLC sessions, use the **no** form of this command.

**source-bridge sdllc-local-ack**

**no source-bridge sdllc-local-ack**

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

## x25 map qllc

To specify the X.121 address of the remote X.25 device with which you plan to communicate using QLLC conversion, use the **x25 map qllc** interface configuration command. To disable QLLC conversion to this X.121 address, use the **no** form of this command.

**x25 map qllc** *virtual-mac-addr x121-addr [x25-map-options]*

**no x25 map qllc** *virtual-mac-addr x121-addr [x25-map-options]*

<b>Syntax Description</b>	<i>virtual-mac-addr</i>	Virtual MAC address.
	<i>x121-addr</i>	X.121 address of the remote X.25 device you are associating with this virtual MAC address. It can be from 1 to 15 digits long.
	<i>x25-map-options</i>	(Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 5.

Table 5 shows the possible values for the *x25-map-options* argument.

Table 5 x.25 map qlc Options

Option	Description
<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 to its impact on overall performance.
<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 uses 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>idle</b> <i>minutes</i>	Specifies an idle timeout for calls other than the interface default; 0 minutes disables the idle timeout.
<b>reverse</b>	Specifies reverse charging for outgoing calls.
<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</b> <i>group-number</i>	Specifies a closed user group number (from 1 to 99) for the mapping in an outgoing call.
<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</i> <i>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.

Table 5 x.25 map qlc Options (continued)

Option	Description
<b>window-size</b> <i>in-size out-size</i>	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.
<b>throughput</b> <i>in out</i>	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</b> <i>milliseconds</i>	Specifies the transit delay value in milliseconds (0 to 65534) for an outgoing call, for networks that support transit delay.
<b>nuid</b> <i>username password</i>	Specifies that a network user ID (NUID) facility be sent in the outgoing call with the specified Terminal Access Controller Access Control System (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.
<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.
<b>roa</b> <i>name</i>	Specifies the name defined by the <b>x25 roa</b> command for a list of transit Recognized Operating Agencies (ROAs) to use in outgoing Call Request packets.
<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.

## x25 pvc qlc

To associate a virtual MAC address with a PVC for communication using QLLC conversion, use the **x25 pvc qlc** interface configuration command. To remove the association, use the **no** form of this command.

```
x25 pvc circuit qlc x121-address [x25-map-options]
```

```
no x25 pvc circuit qlc x121-address [x25-map-options]
```

### Syntax Description

<i>circuit</i>	PVC you are associating with the virtual MAC address. This must be lower than any number assigned to switched virtual circuits.
<i>x121-address</i>	X.121 address.
<i>x25-map-options</i>	(Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 5.





## SNA Frame Relay Access Support Commands

---

This chapter describes the function and syntax of the Systems Network Architecture (SNA) Frame Relay Access Support (FRAS) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### frame-relay map llc2

To configure BSTUN over Frame Relay when using Bisync local acknowledgment, use the **frame-relay map llc2** interface configuration command. To cancel the configuration, use the **no** form of this command.

```
frame-relay map llc2 dlci
```

```
no frame-relay map llc2 dlci
```

---

<b>Syntax Description</b>	<i>dlci</i>	Frame Relay DLCI number on which to support local acknowledgment.
---------------------------	-------------	---

---

### frame-relay map rsrb

To specify the DLCI number onto which the RSRB traffic is to be mapped, use the **frame-relay map rsrb** interface configuration command. To cancel the RSRB map, use the **no** form of this command.

```
frame-relay map rsrb dlci-number
```

```
no frame-relay map rsrb
```

---

<b>Syntax Description</b>	<i>dlci-number</i>	Frame Relay DLCI.
---------------------------	--------------------	-------------------

---

## fras backup dlsw

To configure an auxiliary route between the end stations and the host for use as a backup when the DLCI connection to the Frame Relay network is lost, use the **fras backup dlsw** interface configuration command. To cancel the backup configuration, use the **no** form of this command.

```
fras backup dlsw virtual-mac-address target-ring-number host-mac-address [retry retry-number]
```

```
no fras backup dlsw virtual-mac-address target-ring-number host-mac-address [retry  
retry-number]
```

Syntax Description	
<i>virtual-mac-address</i>	12-digit hexadecimal string used as a source MAC address for all packets going to the host.
<i>target-ring-number</i>	Number configured in the <b>source-bridge ring-group</b> command. This is a virtual ring. The valid range is 1 to 4095.
<i>host-mac-address</i>	Destination MAC address of the host.
<b>retry</b> <i>retry-number</i>	(Optional) Number of attempts by the end station to reconnect to the primary Frame Relay interface before activating the backup link. The range is 1 to 5 retries. If the <b>retry</b> option is not specified, the default number of retries is 5.

## fras ban

To associate bridging over a Frame Relay network using boundary access node (BAN), use the **fras ban** interface configuration command. To cancel each association, use the **no** form of this command.

```
fras ban local-ring bridge-number ring-group ban-dlci-mac dlci dlci#1 [dlci#2 ... dlci#5]  
[bni mac-addr]
```

```
no fras ban local-ring bridge-number ring-group ban-dlci-mac dlci dlci#1 [dlci#2 ... dlci#5]  
[bni mac-addr]
```

Syntax Description	
<i>local-ring</i>	Decimal number from 1 to 4095 describing the Token Ring interface.
<i>bridge-number</i>	Decimal number from 1 to 15 that uniquely identifies a bridge connecting two rings.
<i>ring-group</i>	Decimal number from 1 to 4095 representing a collection of Token Ring interfaces on one or more routers.
<i>ban-dlci-mac</i>	Frame Relay BAN PVC MAC address.
<b>dlci</b> <i>dlci#1</i> [ <i>dlci#2 ... dlci#5</i> ]	Frame Relay DLCI. The <b>dlci</b> keyword precedes the list of one or more DLCI numbers. If you need more than one DLCI number for load balancing, you can configure up to five DLCI numbers, separated by spaces. Each DLCI number must be unique and must be a decimal in the range 16 through 1007.
<b>bni</b> <i>mac-addr</i>	(Optional) Boundary node identifier (BNI) MAC address of the NCP that receives frames from the router.

## fras ddr-backup

To configure an auxiliary interface for use as a backup when the primary Frame Relay link to the Frame Relay WAN fails, use the **fras ddr-backup** interface configuration command. To cancel the backup configuration, use the **no** form of this command.

```
fras ddr-backup interface interface dldci-number
```

```
no fras ddr-backup
```

### Syntax Description

<b>interface</b> <i>interface</i>	Interface over which the backup connection is made.
<i>dldci-number</i>	DLCI number of the session.

## fras-host ban

To enable the FRAS Host function for BAN, use the **fras-host ban** interface configuration command. To disable the FRAS Host BAN functionality, use the **no** form of this command.

```
fras-host ban interface hmac hmac [bni bni]
```

```
no fras-host ban
```

### Syntax Description

<i>interface</i>	Associated Frame Relay interface or subinterface.
<b>hmac</b> <i>hmac</i>	MAC address of the CIP adapter or LAN-attached host.
<b>bni</b> <i>bni</i>	(Optional) Boundary node identifier MAC address. The default <i>bni</i> is 4FFF.0000.0000.

## fras-host bnn

To enable the FRAS Host function for BNN, use the **fras-host bnn** interface configuration command. To disable the FRAS Host function, use the **no** form of this command.

```
fras-host bnn interface fr-lsap sap vmac virt-mac hmac hmac [hsap hsap]
```

```
no fras-host bnn
```

### Syntax Description

<i>interface</i>	Associated Frame Relay interface or subinterface.
<b>fr-lsap</b> <i>sap</i>	LLC2 service access point (SAP). The destination SAP on inbound BNN frames received from Frame Relay.
<b>vmac</b> <i>virt-mac</i>	Used in combination with the DLCI number to form a unique MAC address. The first 4 bytes of the MAC address are formed by the VMAC while the last 2 bytes are formed from the DLCI number. The last 2 bytes of the VMAC must be configured as zeros.

<b>hmac</b> <i>hmac</i>	MAC address of the CIP adapter or LAN-attached host.
<b>hsap</b> <i>hsap</i>	(Optional) Host SAP. If this parameter is not specified, the host SAP value used will match <b>fr-lsap</b> .

## fras-host dlsw-local-ack

To enable LLC2 local termination for FRAS Host connections using the virtual Token Ring, use the **fras-host dlsw-local-ack** interface configuration command. To disable LLC2 local termination, use the **no** form of this command.

**fras-host dlsw-local-ack**

**no fras-host dlsw-local-ack**

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

## fras map llc

To associate an LLC connection with a Frame Relay DLCI, use the **fras map llc** interface configuration command. To disable the association, use the **no** form of this command.

**fras map llc** *lan-lsap* **serial** *interface* **frame-relay dlc** *dlci* *fr-rsap*

**no fras map llc** *lan-lsap* **serial** *interface* **frame-relay dlc** *dlci* *fr-rsap*

<b>Syntax Description</b>	<i>lan-lsap</i>	LLC2 LAN SAP that is the local SAP address of the router.
	<b>serial</b> <i>interface</i>	Serial interface on which Frame Relay is configured.
	<b>frame-relay dlc</b> <i>dlci</i>	Frame Relay DLCI.
	<i>fr-rsap</i>	LLC2 Frame Relay SAP that is the destination SAP of the router on the Frame Relay side.

## fras map sdlc

To associate an SDLC link with a Frame Relay DLCI, use the **fras map sdlc** interface configuration command. To cancel the association, use the **no** form of this command.

**fras map sdlc** *sdlc-address* **serial** *port* **frame-relay dlc** *dlci* *fr-lsap* *fr-rsap* [**pfid2** | **afid2** | **fid4**]

**no fras map sdlc** *sdlc-address* **serial** *port* **frame-relay dlc** *dlci* *fr-lsap* *fr-rsap* [**pfid2** | **afid2** | **fid4**]

<b>Syntax Description</b>	<i>sdlc-address</i>	SDLC address of the downstream SNA device in hexadecimal.
	<b>serial</b> <i>port</i>	Serial interface on which Frame Relay is configured.

<b>frame-relay dlc</b> <i>i</i>	Frame Relay DLCI.
<i>fr-lsap</i>	Local SAP address of the logical link connection on the Cisco Frame Relay Access Device (CFRAD).
<i>fr-rsap</i>	Destination SAP address on the host.
<b>pfid</b>	(Optional) FID2 SNA transmission header for SNA peripheral traffic.
<b>afid2</b>	(Optional) FID2 transmission header for APPN traffic.
<b>fid4</b>	(Optional) Transmission header used on SNA subarea flows.

## interface virtual-tokenring

To create a virtual Token Ring interface, use the **interface virtual-tokenring** interface configuration command. To cancel the configuration, use the **no** form of this command.

```
interface virtual-tokenring number
```

```
no interface virtual-tokenring
```

<b>Syntax Description</b>	<i>number</i>	Number of the virtual Token Ring.
---------------------------	---------------	-----------------------------------

## llc2 dynwind

To enable dynamic window congestion management, use the **llc2 dynwind** interface configuration command. To cancel the configuration, use the **no** form of this command.

```
llc2 dynwind [nw nw-number] [dwc dwc-number]
```

```
no llc2 dynwind [nw nw-number] [dwc dwc-number]
```

<b>Syntax Description</b>	<b>nw</b> <i>nw-number</i>	(Optional) Specifies a number of frames that must be received to increment the working window value by 1. The default is 4.
	<b>dwc</b> <i>dwc-number</i>	(Optional) Specifies the number by which the working window value is divided when BECN occurs. Valid numbers are 1, 2, 4, 8, and 16. 1 is a special value that indicates that the working window value should be set to 1 when BECN is indicated. The default is 1.

## show fras

To view notification that the FRAS dial backup over DLSw+ feature is active, information about the connection state in FRAS, and information about current BNN, BAN, and dial backup, use the **show fras** privileged EXEC command.

```
show fras
```

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

## show fras-host

To display the status of LLC2 sessions using FRAS Host, use the **show fras-host** EXEC command.

```
show fras-host [interface] [dlci dlci-num] [detail]
```

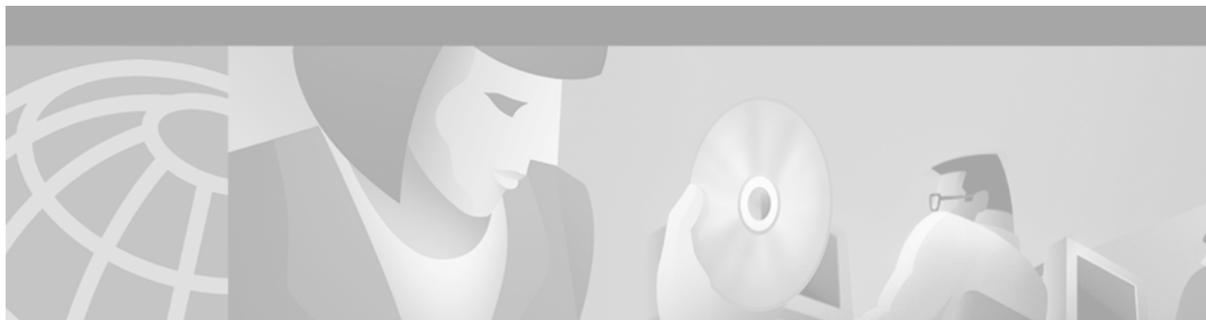
Syntax	Description
<i>interface</i>	(Optional) Only display LLC2 sessions from a specified Frame Relay interface or subinterface.
<b>dlci</b> <i>dlci-number</i>	(Optional) Only display LLC2 sessions from a specified DLCI.
<b>detail</b>	(Optional) Display additional information such as the routing information fields (RIFs) and statistics associated with the LLC2 sessions.

## show fras map

To display the mapping and connection state of FRAS, use the **show fras map** privileged EXEC command.

```
show fras map
```

Syntax	Description
	This command has no arguments or keywords.



## NCIA Client/Server Commands

---

This chapter describes the function and syntax of the native client interface architecture (NCIA) client/server commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### clear ncia circuit

To drop a specified NCIA circuit, use the **clear ncia circuit** privileged EXEC command.

```
clear ncia circuit [id-number]
```

---

**Syntax Description**

*id-number*

(Optional) Number assigned to identify the circuit. If no circuit ID number is specified, the command drops all circuits.

---

### clear ncia client

To terminate a specified active client connection, use the **clear ncia client** privileged EXEC command.

```
clear ncia client [ip-address]
```

---

**Syntax Description**

*ip-address*

(Optional) IP address of the client. If no IP address is specified in the command, the command terminates all active client connections.

---

### clear ncia client registered

To release the control block of a specified registered client after terminating the active connection to it, use the **clear ncia client registered** privileged EXEC command.

```
clear ncia client registered [ip-address]
```

---

**Syntax Description**

*ip-address*

(Optional) IP address of the registered client. If no IP address is specified in the command, the command releases the control blocks of all registered clients after terminating any active connections to them.

---

## ncia

To stop or start an NCIA server, use the **ncia** privileged EXEC command.

**ncia** {**start** | **stop**}

Syntax Description	start	stop
	Starts the NCIA server when it has been stopped using the <b>ncia stop</b> command.	Stops the NCIA server. When the server is stopped, all clients are disconnected, all circuits are dropped, and no clients can connect to the server.

## ncia client

To configure an NCIA client on a Cisco router, use the **ncia client** global configuration command. To remove the configuration, use the **no** form of this command.

**ncia client** *server-number client-ip-address virtual-mac-address* [**sna** | **all**]

**no ncia client** *server-number client-ip-address virtual-mac-address* [**sna** | **all**]

Syntax Description	<i>server-number</i>	<i>client-ip-address</i>	<i>virtual-mac-address</i>	<b>sna</b>	<b>all</b>
	Number assigned to identify the server. Currently, the server number must be configured with a value of 1.	IP address of the client.	Virtual MAC address of the client.	(Optional) NCIA client only supports SNA traffic.	(Optional) NCIA client supports all types of traffic. If you do not specify <b>all</b> as the supported traffic type when you configure an NCIA client, the client supports only SNA traffic.

## ncia rsrb

To configure an RSRB ring to associate with an NCIA server on a Cisco router, use the **ncia rsrb** global configuration command. To remove the configuration, use the **no** form of this command.

**ncia rsrb** *virtual-ring local-bridge local-ring ncia-bridge ncia-ring virtual-mac-address*

**no ncia rsrb**

Syntax Description	<i>virtual-ring</i>	<i>local-bridge</i>	<i>local-ring</i>	<i>ncia-bridge</i>
	RSRB ring group number. This number corresponds to the ring-number parameter defined by a <b>source-bridge ring-group</b> command.	Number of the bridge connecting the virtual ring and the local ring.	Number of the virtual ring connecting the virtual ring and the NCIA ring.	Number of the bridge connecting the local ring and the NCIA ring.

<i>ncia-ring</i>	NCIA ring group number. This number corresponds to the ring-number parameter defined by a <b>source-bridge ring-group</b> command.
<i>virtual-mac-address</i>	Local ring virtual MAC address.

## ncia server

To configure an NCIA server on a Cisco router, use the **ncia server** global configuration command. To remove the configuration, use the **no** form of this command.

```
ncia server server-number server-ip-address server-virtual-mac-address virtual-mac-address
virtual-mac-range [inbound-only] [keepalive seconds] [tcp_keepalive minutes]
```

```
no ncia server
```

Syntax Description	
<i>server-number</i>	Number assigned to identify the server. Currently, the server number must be configured with a value of 1.
<i>server-ip-address</i>	IP address used to accept the incoming connection, or to make an out-going connection.
<i>server-virtual-mac-address</i>	MAC address of the server.
<i>virtual-mac-address</i>	The first MAC address of the virtual MAC address pool.
<i>virtual-mac-range</i>	The range of virtual MAC addresses that can be assigned to the client. The valid range is 1 to 4095. This number sets the upper limit on the number of contiguous MAC addresses that make up the MAC address pool.
<b>inbound-only</b>	(Optional) When <b>inbound-only</b> is configured, the NCIA server cannot make an out-going connection.
<b>keepalive</b> <i>seconds</i>	(Optional) Keepalive interval in seconds. The valid range is 0 to 1200. Setting the value to 0 turns the <b>keepalive</b> off.
<b>tcp_keepalive</b> <i>minutes</i>	(Optional) TCP keepalive processing interval in minutes. The valid range is 0 to 99 minutes. Setting the value to 0 stops TCP from sending keepalive packets when an NCIA client is idle. If no <b>tcp_keepalive</b> value is set, the default waiting period for TCP keepalive packets is 20 minutes.

## show ncia circuits

To display the state of all circuits involving this MAC address as a source and destination, use the **show ncia circuits** privileged EXEC command.

```
show ncia circuits [id-number]
```

Syntax Description	
<i>id-number</i>	(Optional) Number assigned to identify the circuit. If no ID number is specified, the command lists information for all circuits.

## show ncia client

To display the status of the NCIA client, use the **show ncia client** EXEC command.

```
show ncia client [sap-list] [ip-address]
```

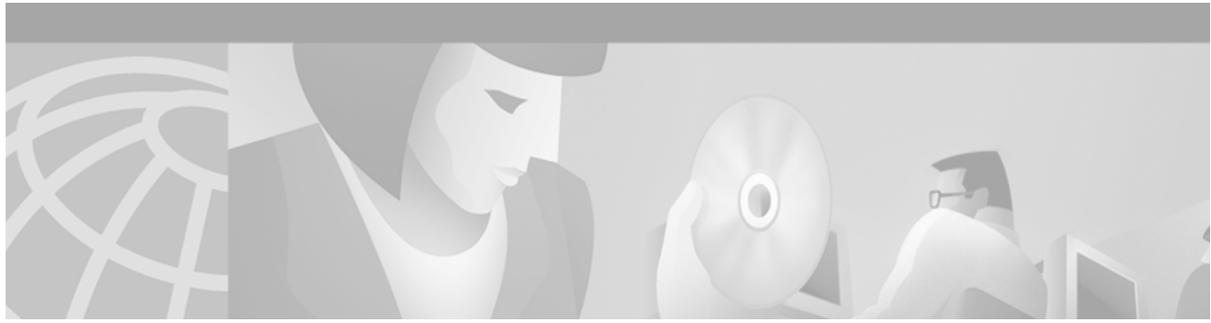
Syntax Description		
	<b>sap-list</b>	(Optional) Display the SAPs supported by the client. If the <b>sap-list</b> option is not specified, the command does not display SAP list information.
	<i>ip-address</i>	(Optional) Client IP address. If no IP address is specified, the command lists information for all clients.

## show ncia server

To display the state of the NCIA server, use the **show ncia server** EXEC command.

```
show ncia server [server-number]
```

Syntax Description		
	<i>server-number</i>	(Optional) NCIA server number. If no server number is specified, the command lists information for all servers.



## Airline Product Set Commands

---

This chapter describes the function and syntax of the Airline Product Set (ALPS) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*.

### alps a1-map a2-map

To specify the A1 and A2 logical ASCU identification information, use the **alps a1-map a2-map** ALPS ASCU submode command. To remove the specification of the A1 and A2 logical ASCU identification information, use the **no** form of this command.

**alps a1-map** *a1-value* **a2-map** *a2-value*

**no alps a1-map** *a1-value* **a2-map** *a2-value*

---

#### Syntax Description

<i>a1-value</i>	A1 logical ASCU identification: <ul style="list-style-type: none"><li>• ALC range—Hexadecimal number in the range 0 to 0xFF.</li><li>• UTS range—Hexadecimal number in the range 0 to 0xFF.</li></ul>
<i>a2-value</i>	A2 logical ASCU identification: <ul style="list-style-type: none"><li>• ALC range—Hexadecimal number in the range 0 to 0xFF.</li><li>• UTS range—Hexadecimal number in the range 0 to 0xFF.</li></ul>

---

## alps alias

To specify that an ALC ASCU is to operate in nonpolling mode, and to specify the parent ASCU interchange address to which this ASCU is aliased, use the **alps alias** ALPS ASCU configuration command. To return the ASCU to polled mode, use the **no** form of this command.

**alps alias** *alias-interchange-address*

**no alps alias** *alias-interchange-address*

---

### Syntax Description

<i>alias-interchange-address</i>	Specifies the interchange address of the polled (alias) ASCU with which to associate this non-polled ASCU. Valid range is between 41 and 7E, except 43, 44, 50 to 53, and 60.
----------------------------------	---

---

## alps ascu

To specify a physical ASCU identity, use the **alps ascu** interface configuration command. To remove the ASCU from the interface and delete any messages queued for transmission to the ASCU or the network, use the **no** form of this command.

**alps ascu** *id*

**no alps ascu** *id*

---

### Syntax Description

<i>id</i>	ASCU identification. Valid range is between 41 and 7E, except 43, 44, 50 to 53, and 60. The UTS valid range is between 21 and 4F.
-----------	---

---

## alps auto-reset

To automatically reset a non-responsive ALC ASCU in the DOWN state, use the **alps auto-reset** ALPS ASCU submode command. To disable the automatic reset, use the **no** form of this command.

**alps auto-reset**

**no alps auto-reset**

---

### Syntax Description

This command has no arguments or keywords.

## alps circuit

To specify an ALPS circuit at the remote CPE across a TCP/IP connection, use the **alps circuit** global configuration command. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

**alps circuit** *name*

**no alps circuit** *name*

---

### Syntax Description

<i>name</i>	Name given to identify an ALPS circuit.
-------------	---

---

## alps connection-type permanent

To specify that this circuit should be established when the circuit is enabled, use the **alps connection-type permanent** ALPS circuit submode command. To remove the permanent activation behavior and return the behavior to the default dynamic activation, use the **no** form of this command.

**alps connection-type permanent** [*retry-timer*]

**no alps connection-type permanent** [*retry-timer*]

---

### Syntax Description

<i>retry-timer</i>	(Optional) Specifies the maximum interval between consecutive attempts to establish a circuit in the event of a failure. The default for <i>retry-timer</i> is 30 seconds and the range is 1 to 180 seconds.
--------------------	--

---

## alps default-circuit

To specify the ALPS circuit that this ASCU uses, use the **alps default-circuit** ALPS ASCU submode command. To remove the default circuit specification, use the **no** form of this command.

**alps default-circuit** *name*

**no alps default-circuit** *name*

---

### Syntax Description

<i>name</i>	Name given to identify an ALPS circuit on the remote CPE.
-------------	---

---

## alps enable-alarms ascu

To enable alarms for the ALPS ASCUs, use the **alps enable-alarms ascu** global configuration command at the remote CPE. To disable alarms for the ALPS ASCUs, use the **no** form of this command.

**alps enable-alarms ascu** [*interface id*]

**no alps enable-alarms ascu**

---

<b>Syntax Description</b>	<i>interface id</i> (Optional) ASCU identifier. Enable alarms for the specified ASCU.
---------------------------	---

---

## alps enable-alarms circuit

To enable alarms for the ALPS circuits, use the **alps enable-alarms circuit** global configuration command. To remove the circuit definition from the configuration, use the **no** form of this command.

**alps enable-alarms circuit** [*name*]

**no alps enable-alarms circuit** [*name*]

---

<b>Syntax Description</b>	<i>name</i> (Optional) Name given to identify an ALPS circuit on the remote CPE.
---------------------------	--

---

## alps enable-alarms peer

To enable alarms for the ALPS peers, use the **alps enable-alarms peer** global configuration command. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

**alps enable-alarms peer** [*ip-address*]

**no alps enable-alarms peer** [*ip-address*]

---

<b>Syntax Description</b>	<i>ip-address</i> (Optional) IP address of the remote peer for which alarms are enabled.
---------------------------	--

---

## alps enable-ascu

To move the previously defined ASCU from the inactive poll list to the active poll list, use the **alps enable-ascu** ALPS ASCU submode command. This move results in the protocol handler polling the ASCU and rendering it ready for handling terminal traffic. To remove the ASCU from the active poll list to the inactive poll list, use the **no** form of this command. This action prevents the ASCU from being polled, rendering it not ready for handling terminal traffic.

**alps enable-ascu**

**no alps enable-ascu**

---

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

## alps enable-circuit

To enable the circuit to be activated when data is received from an ASCU, use the **alps enable-circuit** ALPS circuit submode command. To disable the circuit, use the **no** form of this command.

**alps enable-circuit**

**no alps enable-circuit**

---

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

## alps error-display

To specify where error messages about service availability or network problems are displayed, use the **alps error-display** ALPS ASCU submode command. To return to the default values, use the **no** form of this command.

**alps error-display** *number1* *number2*

**no alps error-display** *number1* *number2*

---

<b>Syntax Description</b>	<i>number1</i>	For P1024B ALC, specifies the terminal address where these service messages are sent. Valid numbers are hexadecimal numbers in the range 0x40 to 0x7F. The default address is 0x72.
		For P1024C UTS, specifies the screen line number where service messages are displayed. Valid numbers are hexadecimal numbers in the range 0x00 to 0x7F. The default line number is 0x37.

---

<i>number2</i>	For P1024B ALC, specifies the screen line number where service messages are displayed. Valid numbers are hexadecimal numbers in the range 0x40 to 0x7F. The default screen line number is 0x66.  For P1024C UTS, specifies the column number where service messages are displayed. Valid numbers are hexadecimal numbers in the range 0x00 to 0x7F. The default column number is 0x20.
----------------	--

## alps host-hld host-link

To enable ALPS on the X.25 interface, use the **alps host-hld host-link** interface configuration command. To disable ALPS on the X.25 interface, use the **no** form of this command.

```
alps host-hld hld host-link number {{ax25 [damp-tmr value]} | emtox x.121 [pseudo-conv]} [life-tmr value]
```

```
no alps host-hld hld host-link number {{ax25 [damp-tmr value]} | emtox x.121 [pseudo-conv]} [life-tmr value]
```

### Syntax Description

<i>hld</i>	Host high-level designator. A hexadecimal number in the range 1 to 7f7f.
<i>number</i>	Host-link identifier. A number in the range 1 to 255.
<b>ax25</b>	Specifies airline X.25 implementation of X.25.
<b>damp-tmr</b> <i>value</i>	(Optional) Specifies the AX.25 PVC damping timer. The <i>value</i> argument is the length of time that a PVC can be inactive before it is destroyed and the corresponding ALPS circuits are closed. The default is 10 seconds.
<b>emtox</b>	Specifies EMTOX implementation of X.25.
<i>x.121</i>	X.121 address of the EMTOX host (called address on calls to the EMTOX host).
<i>pseudo-conv</i>	(Optional) Specifies the pseudo-conversational format of EMTOX packets.
<b>life-tmr</b> <i>value</i>	(Optional) Specifies the maximum amount of time (in seconds) that a message may be queued for sending to the host X.25 system before it is discarded. The <i>value</i> argument is time (in seconds).

## alps hostlink

To specify information required to establish an X.25 virtual circuit at the central CPE, use the **alps hostlink** ALPS circuit submode command. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

```
alps hostlink number {ax25 lcn | emtox x121-address} [winout val1] [winin val2] [ops val3] [ips val4]
```

```
no alps hostlink number {ax25 lcn | emtox x121-address} [winout val1] [winin val2] [ops val3] [ips val4]
```

Syntax Description		
	<i>number</i>	Interface at the host CPE. Decimal number in the range 1 to 255.
	<b>ax25</b>	Specifies airline X.25 implementation of X.25.
	<i>lcn</i>	Local channel number for AX.25 connections.
	<b>emtox</b>	Specifies EMTOX implementation of X.25.
	<i>x121-address</i>	X.121 address for EMTOX connections. This is the X.121 calling address for X.25 call packets sent from the central CPE to the EMTOX host. This address is the source address in a call to the host.
	<b>winout</b> <i>val1</i>	(Optional) Specifies the X.25 send window. The <i>val1</i> argument is a decimal number in the range 1 to 7.
	<b>winin</b> <i>val2</i>	(Optional) Specifies the X.25 receive window. The <i>val2</i> argument is a decimal number in the range 1 to 7.
	<b>ops</b> <i>val3</i>	(Optional) Specifies the maximum output packet size. The <i>val3</i> argument is one of the following numbers: 128, 240, 256, 512, 1024, 2048, or 4096.
	<b>ips</b> <i>val4</i>	(Optional) Specifies the maximum input packet size. The <i>val4</i> argument is one of the following numbers: 128, 240, 256, 512, 1024, 2048, or 4096.

## alps idle-timer

To specify (for dynamic circuits) the length of time that can elapse before an idle circuit is disabled, use the **alps idle-timer** ALPS circuit submode command. To return to the default idle-timer value, use the **no** form of this command.

**alps idle-timer** *timer*

**no alps idle-timer** *timer*

Syntax Description	<i>timer</i>	Length of time that can elapse before an idle circuit is brought down. The range is 10 to 600 seconds. The default is 60 seconds.

## alps keepalive

To enable TCP keepalives for ALPS TCP peer connections, use the **alps keepalive** global configuration command. A TCP keepalive request will be sent to the remote peer if the TCP connection to the remote peer is silent for a time period larger than the interval specified. The TCP connection to the ALPS host will be closed when a count equal to the retry count specified is missed consecutively. To disable keepalives for ALPS, use the **no** form of this command.

**alps keepalive** [*interval time*] [*retry count*]

**no alps keepalive** [*interval time*] [*retry count*]

Syntax Description		
<b>interval</b> <i>time</i>	(Optional) Interval for keepalive requests. The <i>time</i> argument is the keepalive interval, in the range of 10 to 300 seconds. The default is 30 seconds.	
<b>retry</b> <i>count</i>	(Optional) Indicates how many times keepalive requests will be sent before the connection is closed. The <i>count</i> argument is the retry count, in the range 1 to 10. The default is 3 retries.	

## alps lifetime-timer

To specify how long messages can be queued in the ALPS circuit queue awaiting transmission to the central CPE, use the **alps lifetime-timer** ALPS circuit submode command. To return to the default lifetime-timer value, use the **no** form of this command.

**alps lifetime-timer** *timer*

**no alps lifetime-timer** *timer*

Syntax Description	<i>timer</i>	
		Length of time, in seconds, that a message can be queued. The range is 1 to 20 seconds. The default is 4 seconds.

## alps local-hld remote-hld

To specify the local and remote HLDs to use for this ALPS circuit, use the **alps local-hld remote-hld** ALPS circuit submode command. To remove the definition from the configuration, use the **no** form of this command.

**alps local-hld** *loc-hld* **remote-hld** *rem-hld*

**no alps local-hld** *loc-hld* **remote-hld** *rem-hld*

Syntax Description	<i>loc-hld</i>	
		Local HLD to use for ALPS circuit. Hexadecimal number in the range 1 to FFFF.
	<i>rem-hld</i>	Remote HLD to use for ALPS circuit. Hexadecimal number in the range 1 to FFFF.

## alps local-peer

To specify the IP address of the local peer, use the **alps local-peer** global configuration command. To remove all subsequent ALPS configuration commands from the router, use the **no** form of this command.

**alps local-peer** *ip-address* [**promiscuous**]

**no alps local-peer** *ip-address* [**promiscuous**]

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the local peer.
	<b>promiscuous</b>	(Optional) Keyword specified at the central CPE to accept incoming TCP connections from any remote CPE.

## alps matip-close-delay

To specify the interval between the closing and reopening of MATIP circuit connections, use the **alps matip-close-delay** ALPS circuit submode command. To restore the definition to the default value, use the **no** form of this command.

**alps matip-close-delay** *time*

**no alps matip-close-delay** *time*

<b>Syntax Description</b>	<i>time</i>	Minimum number of seconds between the closing and reopening of an ALPS MATIP circuit. The range is 1 to 90 seconds. The default is 10 seconds.
---------------------------	-------------	--

## alps max-msg-length

To specify maximum input message length, use the **alps max-msg-length** ALPS ASCU submode command. To return to the default maximum input message length, use the **no** form of this command.

**alps max-msg-length** *value*

**no alps max-msg-length** *value*

<b>Syntax Description</b>	<i>value</i>	Maximum input message length. The range is 1 to 3840. The default is 962 characters.
---------------------------	--------------	--

## alps mpx

To specify the multiplexing and the ASCU identification header for this circuit, use the **alps mpx** ALPS circuit submode command. To remove the definition from the configuration, use the **no** form of this command.

**alps mpx** {*group* | *single*} **hdr** {*a1a2* | *none*}

**no alps mpx** {*group* | *single*} **hdr** {*a1a2* | *none*}

<b>Syntax Description</b>	<b>group</b>	Specifies that multiple ASCUs will be multiplexed on the ALPS circuit. This setting is the default.
	<b>single</b>	Specifies that only one ASCU will use this circuit.

<b>hdr</b>	Specifies the ASCU identification header for the circuit. The default is a1a2.
<b>a1a2</b>	ASCU identification via A1, A2.
<b>none</b>	No ASCU identification.

## alps n1

To specify the threshold of consecutive errors logged before an ASCU is declared down, use the **alps n1** interface configuration command. To reassert the default number of consecutive errors before declaring an ASCU down, use the **no** form of this command.

**alps n1** *errors*

**no alps n1** *errors*

### Syntax Description

<i>errors</i>	Error count limit. The valid range is 1 to 30 errors. The default for ALC is 30 errors. The default for UTS is 10 errors.
---------------	---

## alps n2

To specify the number of polls that must be correctly replied to before an ASCU is declared up, use the **alps n2** interface configuration command. To reassert the default number of polls that must be correctly replied before an ASCU is declared up, use the **no** form of this command.

**alps n2** *polls*

**no alps n2** *polls*

### Syntax Description

<i>polls</i>	Number of polls that must be correctly replied to. The valid range is 1 to 30 polls. The default is 1 poll.
--------------	---

## alps n3

To specify the maximum number of retransmissions of an unacknowledged output data message to an ASCU, use the **alps n3** interface configuration command. To reassert the default, use the **no** form of this command.

**alps n3** *value*

**no alps n3** *value*

### Syntax Description

<i>value</i>	Maximum number of times an unacknowledged output data message can be resent. When the number is exceeded the output data message is dropped. The valid range is 1 to 10 resends. The default is 3 resends.
--------------	--

## alps poll-pause

To set the minimum interval, in milliseconds, between two polls to the same ASCU, use the **alps poll-pause** interface configuration command. To the default interval, use the **no** form of this command to revert.

```
alps poll-pause msec
```

```
no alps poll-pause
```

### Syntax Description

<i>msec</i>	Minimum interval between polls, in milliseconds. The valid range is 10 to 1000 ms. The default interval is 50 ms.
-------------	---

## alps primary-peer

To specify the primary TCP peer and, optionally, a backup TCP peer for an ALPS circuit, use the **alps primary-peer** ALPS circuit submode command. To remove the definition from the configuration, use the **no** form of this command.

```
alps primary-peer ip-address [backup-peer ip-address]
```

```
no alps primary-peer ip-address [backup-peer ip-address]
```

### Syntax Description

<i>ip-address</i>	IP address specified in the <b>alps remote-peer</b> command.
<b>backup-peer</b>	(Optional) Backup TCP peer for the ALPS circuit.
<i>ip-address</i>	(Optional) IP address specified in the <b>alps remote-peer</b> command.

## alps remote-peer

To specify the partner IP address for an ALPS circuit, use the **alps remote-peer** global configuration command. To remove the definition from the configuration, use the **no** form of this command.

```
alps remote-peer ip-address [protocol { atp | matip-a }] [status-interval interval] [status-retry retries] [dynamic [inact-timer] [no-circuit no-circ-timer]] [tcp-qlen [number]]
```

```
no alps remote-peer ip-address [protocol { atp | matip-a }] [status-interval interval] [status-retry retries] [dynamic [inact-timer] [no-circuit no-circ-timer]] [tcp-qlen [number]]
```

### Syntax Description

<i>ip-address</i>	IP address of the peer.
<b>protocol { atp   matip-a }</b>	(Optional) Specifies the type of encapsulation for the connection. The following options are available: <ul style="list-style-type: none"> <li>ALPS Tunneling Protocol encapsulation. This encapsulation is the default.</li> <li>MATIP Type A (conversational) encapsulation.</li> </ul>

<b>status-interval</b> <i>interval</i>	(Optional) Specifies amount of time, in seconds, between sending of MATIP status messages. The messages verify the integrity of the TCP connection. Number of seconds between status messages. The range is 0 to 300 seconds. The default value is 0 (off).
<b>status-retry</b> <i>retries</i>	(Optional) Specifies number of times to retry sending a MATIP status message before the peer connection is closed. Number of retries. The range is 0 to 100 retries. The default value is 2.
<b>dynamic</b> <i>inact-timer</i>	(Optional) Allows the TCP connection to the host peer to be opened only when there is data to be transferred to the host reservation system. Length of inactivity, in seconds, after which the connection is closed. The range is 0 to 300 seconds. The default is 30 seconds. A value of zero indicates that the timer is disabled.
<b>no-circuit</b> <i>no-circ-timer</i>	(Optional) Specifies amount of time, in seconds, that a peer will stay connected while no circuits are using the peer connection. This parameter is valid only if the dynamic parameter is first configured. Number of seconds before which the timer will expire. The range is 0 to 3600 seconds. The default is 90 seconds.
<b>tcp-qlen</b> <i>number</i>	(Optional) Specifies the maximum length of a TCP queue for peer connections. Number of packets allowed in the TCP queue. The range is 26 to 100 packets. The default is 50 packets.

## alps retry-option

To configure the CPE to signal the ASCU whenever an error is detected, use the **alps retry-option** ALPS ASCU submode command. To reassert the default action of no retry, use the **no** form of this command.

**alps retry-option** { **resend** | **reenter** }

**no alps retry-option**

Syntax Description	
<b>resend</b>	Specifies the retry option as resend. This option causes an indicator LED to signal the operator at the ASCU to resend data.
<b>reenter</b>	Specifies the retry option as reenter. This option causes a service message to signal the operator at the ASCU to reenter data.

## alps service-msg-interval

To specify the interval between consecutive transmissions of service messages from the remote CPE to the ASCU, use the **alps service-msg-interval** ALPS circuit submode command. To remove the definition from the configuration, use the **no** form of this command.

**alps service-msg-interval** *seconds*

**no alps service-msg-interval** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Interval, in seconds, between consecutive sendings of service messages from the remote CPE to the ASCU. The range is 1 to 20 seconds. The default interval is 4 seconds.
---------------------------	----------------	--

## alps service-msg-list

To define the service message list to be used for this circuit, use the **alps service-msg-list** ALPS circuit submode command. To remove the list from the circuit configuration, thus issuing no service messages until another list is configured, use the **no** form of this command.

**alps service-msg-list** *list*

**no alps service-msg-list** *list*

<b>Syntax Description</b>	<i>list</i>	The service message list to be used for this circuit. The valid numbers are 1 to 8.
---------------------------	-------------	---

## alps service-msg-list number

To define the service message identity and its contents for a service message list, use the **alps service-msg-list number** global configuration command. To remove a service message number from the service message list configuration, use the **no** form of this command.

**alps service-msg-list** *list number number message*

**no alps service-msg-list** *list number number message*

<b>Syntax Description</b>	<i>list</i>	Service message list to be used for this circuit. Valid numbers are 1 to 8.
	<i>number</i>	List number. Valid numbers are 1 to 8.
	<i>message</i>	Contents of a service message. Maximum number of characters allowed in a service message is 32.



**Note** Configuring the *message* argument with a value of \$OFF\$ disables this particular service message.

## alps service-msg data-drop

To specify where to retrieve the terminal address to be used when a service message is sent to an ASCU as the result of a dropped data message, use the **alps service-msg data-drop** interface configuration command. To remove the terminal address specification, use the **no** form of this command.

```
alps service-msg data-drop {msg-term | config-term}
```

```
no alps service-msg data-drop {msg-term | config-term}
```

Syntax Description	msg-term	Specifies that the service message will be sent to the terminal address of the dropped message.
	config-term	Specifies that the service message terminal address is the same address configured in the <b>alps-error display</b> command.

## alps service-msg format

To specify the protocol format of service messages sent from the router to an ASCU, use the **alps service-msg format** interface configuration command. To remove the protocol format specification, use the **no** form of this command.

```
alps service-msg format {sita | apollo}
```

```
no alps service-msg format {sita | apollo}
```

Syntax Description	sita	Specifies the <b>sita</b> protocol format.
	apollo	Specifies the <b>apollo</b> protocol format.

## alps service-msg status-change

To specify that service messages for ALPS circuit status changes be sent to ASCUs on the serial interface, use the **alps service-msg status-change** interface configuration command. To send service messages for ALPS circuit status changes only when ALC data messages are dropped, use the **no** form of this command.

```
alps service-msg status-change
```

```
no alps service-msg status-change
```

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

## alps servlim

To specify the number of polls of the ASCU UP list allowed between two successive polls of the ASCU DOWN list, use the **alps servlim** interface configuration command. To reassert the default number of cycles through the normal (active) poll list allowed before the slow poll list is processed, use the **no** form of this command.

**alps servlim** *polls*

**no alps servlim** *polls*

---

### Syntax Description

<i>polls</i>	Number of polls of the ASCU UP list. The valid range is 1 to 512 polls. The default is 30 polls.
--------------	--

---

## alps t1

To specify the timeout delay between polling and response, use the **alps t1** interface configuration command. To reassert the default poll timeout value of 0.5 seconds, use the **no** form of this command.

**alps t1** *delay*

**no alps t1** *delay*

---

### Syntax Description

<i>delay</i>	Timeout delay, in seconds, between polling and response. The valid range is 1 to 20 tenths of a second (0.1 to 2 seconds). The default is 5 tenths of a second (0.5 second).
--------------	--

---

## alps t2

To specify the timeout delay between receipt of the first character of an I/P sequence solicited by a poll and receipt of a Go Ahead (GA) sequence, use the **alps t2** interface configuration command. To reassert the default timeout value of 6 seconds, use the **no** form of this command.

**alps t2** *delay*

**no alps t2** *delay*

---

### Syntax Description

<i>delay</i>	Timeout delay, in seconds, between receipt of first character of an I/P sequence solicited by a poll and receipt of Go Ahead (GA) sequence. The valid range is 1 to 10 seconds. The default is 6 seconds.
--------------	---

---

## alps translate

To map an X.121 address to an IP address of a remote peer, use the **alps translate** interface configuration command. To remove mapping from the configuration, use the **no** form of this command.

```
alps translate x.121-address ip-address
```

```
no alps translate x.121-address ip-address
```

Syntax Description		
	<i>x.121-address</i>	X.121 address to be mapped to an IP address of a remote peer.
	<i>ip-address</i>	IP address of the remote peer.

## alps update-circuit

To update one or more ALPS circuits, use the **alps update-circuit** EXEC command. If a circuit name is specified, then only that circuit will be updated; otherwise, all circuits will be updated.

```
alps update-circuit [name]
```

Syntax Description		
	<i>name</i>	(Optional) Specifies name of circuit to update.

## clear alps circuits

To remove configured ALPS circuits, use the **clear alps circuits** EXEC command.

```
clear alps circuits [ipaddr address | name string]
```

Syntax Description		
	<b>ipaddr</b> <i>address</i>	(Optional) Clear ALPS circuits for peer with specified IP address.
	<b>name</b> <i>string</i>	(Optional) Clear ALPS circuits for peer with specified name.

## clear alps counters

To clear all counters relevant to the ALPS feature, use the **clear alps counters** EXEC command.

```
clear alps counters
```

Syntax Description	
	This command has no arguments or keywords.

## encapsulation alc

To specify that the P1024B Airline Control (ALC) protocol will be used on the serial interface, use the **encapsulation alc** interface configuration command. To remove ALC protocol handling from the serial interface, and return the default encapsulation (HDLC) to the interface, use the **no** form of this command.

**encapsulation alc**

**no encapsulation alc**

---

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

## encapsulation uts

To specify that the P1024C Universal Terminal Support (UTS) protocol will be used on the serial interface, use the **encapsulation uts** interface configuration command. To remove P1024C UTS protocol handling from the serial interface and return the default encapsulation (HDLC) to the interface, use the **no** form of this command.

**encapsulation uts**

**no encapsulation uts**

---

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

## show alps ascu

To display the status of the ALPS ASCU, use the **show alps ascu EXEC** command.

**show alps ascu** [*interface* [*id*]] [**detail**]

---

<b>Syntax Description</b>	<i>interface</i> [ <i>id</i> ]	(Optional) Combined interface and ASCU interchange address (IA). If the interface and ASCU are specified, the status for only the ASCU on that interface is displayed. If only the interface is specified, all ASCUs defined on that interface are displayed. If the interface and ASCU are not specified, then all ASCUs defined are displayed.
	<b>detail</b>	(Optional) Displays detailed output.

---

## show alps circuits

To display the status of the ALPS circuits, use the **show alps circuits** EXEC command. If a circuit name is specified, then only the status of that circuit will be displayed; otherwise, the status of all circuits will be displayed.

**show alps circuits** [*peer ipaddress*] [*name name*] [**detail**]

### Syntax Description

<b>peer</b> <i>ipaddress</i>	(Optional) Displays the status of the circuits connected to the specified peer.
<b>name</b> <i>name</i>	(Optional) Displays only the status of that circuit.
<b>detail</b>	(Optional) Displays detailed output.

## show alps peers

To display the status of the ALPS partner peers, use the **show alps peers** EXEC command. If an IP address is specified, then only the status of that peer will be displayed; otherwise, the status of all peers will be displayed.

**show alps peers** [*ipaddress address*] [**detail**]

### Syntax Description

<b>ipaddress</b> <i>address</i>	(Optional) Displays only the status of that ASCU.
<b>detail</b>	(Optional) Displays detailed output.



**Bridging and IBM Networking  
Volume 2 of 2**





## DSPU and SNA Service Point Commands

---

This chapter describes the function and syntax of the downstream physical unit (DSPU) and Systems Network Architecture (SNA) Service Point commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*.

### dspu activation-window

To define the number of activation request units (RUs) and response messages (such as ACTLUs or DDDLUs NMVTs) that can be sent without waiting for responses from the remote PU, use the **dspu activation-window** global configuration command. To restore the default window size, use the **no** form of this command.

```
dspu activation-window window-size
```

```
no dspu activation-window
```

---

<b>Syntax Description</b>	<i>window-size</i>	Number of outstanding unacknowledged activation RUs. The default is 5.
---------------------------	--------------------	--

---

### dspu default-pu

To enable the default PU feature to be used when a downstream PU attempts to connect, but does not match any of the explicit PU definitions, use the **dspu default-pu** global configuration command. To disable the default PU feature, use the **no** form of this command.

```
dspu default-pu [window window-size] [maxiframe max-iframe]
```

```
no dspu default-pu [window window-size] [maxiframe max-iframe]
```

---

<b>Syntax Description</b>	<b>window</b> <i>window-size</i>	(Optional) Send and receive window sizes used across the link. The range is 1 to 127. The default is 7.
	<b>maxiframe</b> <i>max-iframe</i>	(Optional) Maximum size (in bytes) of an I-frame that can be sent or received across the link. The range is 64 bytes to 18,432 bytes. The default is 1472.

---

## dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)

To enable a local SAP on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts, use the **dspu enable-host** interface configuration command. To cancel the definition, use the **no** form of this command.

**dspu enable-host** [*lsap local-sap*]

**no dspu enable-host** [*lsap local-sap*]

<b>Syntax Description</b>	<b>lsap</b>	(Optional) Specifies that the local SAP will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts.
	<i>local-sap</i>	(Optional) Local SAP address. The default is 12.

## dspu enable-host (QLLC)

To enable an X.121 subaddress for use by upstream host connections via QLLC, use the **dspu enable-host** interface configuration command. To disable the X.121 subaddress, use the **no** form of this command.

**dspu enable-host qlc** *x121-subaddress*

**no dspu enable-host qlc** *x121-subaddress*

<b>Syntax Description</b>	<b>qlc</b>	Required keyword for QLLC data-link control.
	<i>x121-subaddress</i>	X.121 subaddress.

## dspu enable-host (SDLC)

To enable an SDLC address for use by upstream host connections, use the **dspu enable-host** interface configuration command. To cancel the definition, use the **no** form of this command.

**dspu enable-host sdlc** *sdlc-address*

**no dspu enable-host sdlc** *sdlc-address*

<b>Syntax Description</b>	<b>sdlc</b>	Required keyword for SDLC data-link control.
	<i>sdlc-address</i>	SDLC address.

## dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)

To enable an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstream PU connections, use the **dspu enable-pu** interface configuration command. To disable the connection, use the **no** form of this command.

**dspu enable-pu** [*lsap local-sap*]

**no dspu enable-pu** [*lsap local-sap*]

<b>Syntax Description</b>	<i>lsap local-sap</i>	(Optional) Local SAP address used by the DSPU to establish connection with the remote host. The default local SAP address is 8.
---------------------------	-----------------------	---

## dspu enable-pu (QLLC)

To enable an X.121 subaddress for use by downstream PU connections via QLLC, use the **dspu enable-pu** interface configuration command. To cancel the definition, use the **no** form of this command.

**dspu enable-pu qlc** *x121-subaddress*

**no dspu enable-pu qlc** *x121-subaddress*

<b>Syntax Description</b>	<b>qlc</b>	Required keyword for QLLC data-link control.
	<i>x121-subaddress</i>	Variable-length X.121 address. It is assigned by the X.25 network service provider.

## dspu enable-pu (SDLC)

To enable an SDLC address for use by downstream PU connections, use the **dspu enable-pu** interface configuration command. To disable the connection, use the **no** form of this command.

**dspu enable-pu sdlc** *sdlc-address*

**no dspu enable-pu sdlc** *sdlc-address*

<b>Syntax Description</b>	<b>sdlc</b>	Required keyword for SDLC data-link control.
	<i>sdlc-address</i>	SDLC address.

## dspu host (Frame Relay)

To define a DSPU host over a Frame Relay connection, use the **dspu host** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu host host-name xid-snd xid dlci dlci-number [rsap rsap-addr] [lsap lsap-addr]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

```
no dspu host host-name xid-snd xid dlci dlci-number [rsap remote-sap] [lsap local-sap]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

### Syntax Description

<b>host-name</b>	The specified DSPU host.
<b>xid-snd</b> <i>xid</i>	XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
<b>dlci</b> <i>dlci-number</i>	Frame Relay data-link connection identifier (DLCI) number; a decimal number.
<b>rsap</b> <i>rsap-addr</i>	(Optional) Remote service access point (SAP) address.
<b>lsap</b> <i>lsap-addr</i>	(Optional) Local SAP address.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive window sizes used for the host link. The range is 1 to 127.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>	(Optional) Specifies that the host link will be used for the focal point support.

## dspu host (QLLC)

To define a DSPU host over an X.25/QLLC connection, use the **dspu host** global configuration command. To delete the DSPU host definition, use the **no** form of this command.

```
dspu host host-name xid-snd xid x25 remote-x121-addr [qllc local-x121-subaddr]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

```
no dspu host host-name xid-snd xid x25 remote-x121-addr [qllc local-x121-subaddr]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

### Syntax Description

<i>host-name</i>	The specified DSPU host.
<b>xid-snd</b> <i>xid</i>	XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the Block number is 05D and the ID number is 00001.
<b>x25</b> <i>remote-x121-addr</i>	Remote X.121 address.
<b>qllc</b> <i>local-x121-subaddr</i>	(Optional) Local X.121 subaddress.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive window sizes used for the host link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>	(Optional) Specifies that the host link will be used for the focal point support.

## dspu host (SDLC)

To define a DSPU host over an SDLC connection, use the **dspu host** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu host host-name xid-snd xid sdlc sdlc-addr [interface slot/port] [window window-size]
[maxiframe max-iframe] [retries retry-count] [retry-timeout retry-timeout] [focalpoint]
```

```
no dspu host host-name xid-snd xid sdlc sdlc-addr [interface slot/port] [window window-size]
[maxiframe max-iframe] [retries retry-count] [retry-timeout retry-timeout] [focalpoint]
```

Syntax Description		
<i>host-name</i>		The specified DSPU host.
<b>xid-snd</b> <i>xid</i>		XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both Block and ID numbers. For example, if the XID value is 05D00001, the Block number is 05D and the ID number is 00001.
<b>sdlc</b> <i>sdlc-addr</i>		SDLC hexadecimal address.
<b>interface</b> <i>slot/port</i>		(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>		(Optional) Send and receive window sizes used for the host link. The range is 1 to 127. The default window size is 7.
<b>maxiframe</b> <i>max-iframe</i>		(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>		(Optional) Number of times the DSPU attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
<b>retry-timeout</b> <i>retry-timeout</i>		(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>		(Optional) Specifies that the host link will be used for the focal point support.

## dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)

To define a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections, use the **dspu host** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu host host-name xid-snd xid rmac remote-mac [rsap remote-sap] [lsap local-sap]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

```
no dspu host host-name xid-snd xid rmac remote-mac [rsap remote-sap] [lsap local-sap]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

Syntax Description		
<i>host-name</i>		The specified DSPU host.
<b>xid-snd</b> <i>xid</i>		XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both Block and ID numbers. For example, if the XID value is 05D00001, the Block number is 05D and the ID number is 00001.
<b>rmac</b> <i>remote-mac</i>		MAC address of the remote host PU.
<b>rsap</b> <i>remote-sap</i>		(Optional) SAP address of the remote host PU. The default is 4.
<b>lsap</b> <i>local-sap</i>		(Optional) Local SAP address used by the DSPU to establish connection with the remote host. The default is 12.
<b>interface</b> <i>slot/port</i>		(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>		(Optional) Send and receive window sizes used for the host link. The range is 1 to 127. The default is 7.

<b>maxiframe</b> <i>max-iframe</i>	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>	(Optional) Specifies that the host link will be used for the focal point support.

## dspu lu

To define a dedicated LU or a range of LUs for an upstream host and a downstream PU, use the **dspu lu** global configuration command. To cancel the definition, use the **no** form of this command.

**dspu lu** *lu-start* [*lu-end*] {**host** *host-name host-lu-start* | **pool** *pool-name*} [**pu** *pu-name*]

**no dspu lu** *lu-start* [*lu-end*] {**host** *host-name host-lu-start* | **pool** *pool-name*} [**pu** *pu-name*]

### Syntax Description

<i>lu-start</i>	Starting LU address in the range of LUs to be assigned from a pool or dedicated to a host.
<i>lu-end</i>	(Optional) Ending LU address in the range of LUs to be assigned from a pool or dedicated to a host.
<b>host</b> <i>host-name host-lu-start</i>	Specifies that each LU in the range of LUs will be dedicated to a host LU <i>host-name</i> . The range of host LUs starts with the address <i>host-lu-start</i> .
<b>pool</b> <i>pool-name</i>	Specifies that each LU in the range of LUs will be assigned from the specified pool.
<b>pu</b> <i>pu-name</i>	(Optional) Downstream PU for which this range of LUs is being defined.

## dspu ncia

To configure the NCIA server as the underlying transport, use the **dspu ncia** global configuration command. To cancel the definition, use the **no** form of this command.

**dspu ncia** [*server-number*]

**no dspu ncia** [*server-number*]

### Syntax Description

<i>server-number</i>	(Optional) Server number configured in the <b>ncia server</b> command. Currently, only one NCIA server is supported.
----------------------	--

## dspu ncia enable-pu

To enable a SAP on the NCIA server for use by downstream connections, use the **dspu ncia enable-pu** global configuration command. To disable the SAP, use the **no** form of this command.

**dspu ncia enable-pu** [**lsap** *local-sap*]

**no dspu ncia enable-pu** [**lsap** *local-sap*]

### Syntax Description

<b>lsap</b> <i>local-sap</i>	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for receiving incoming connection attempts. The default is 8.
------------------------------	--

## dspu notification-level

To specify the DSPU notifications to send to SNMP and SNA network management, use the **dspu notification-level** global configuration command. To specify the default notification level **low**, use the **no** form of this command.

**dspu notification-level** { **off** | **low** | **medium** | **high** }

**no dspu notification-level**

### Syntax Description

<b>off</b>	Sends neither SNMP traps nor unsolicited SNA messages for DSPU.
<b>low</b>	Sends PU and LU activation failures only.
<b>medium</b>	Sends PU state changes and PU and LU activation failures.
<b>high</b>	Sends both PU and LU state changes and activation failures.

## dspu pool

To define a range of host LUs in an LU pool, use the **dspu pool** global configuration command. To remove the definition, use the **no** form of this command.

**dspu pool** *pool-name* **host** *host-name* **lu** *lu-start* [*lu-end*] [**inactivity-timeout** *minutes*]

**no dspu pool** *pool-name* **host** *host-name* **lu** *lu-start* [*lu-end*] [**inactivity-timeout** *minutes*]

### Syntax Description

<i>pool-name</i>	Name identifier of the pool.
<b>host</b> <i>host-name</i>	Name of the host that owns the range of host LUs in the pool.
<b>lu</b> <i>lu-start</i>	Starting LU address in the range of host LUs in the pool.
<i>lu-end</i>	(Optional) Ending address (inclusive) of the range of host LUs in the pool. If no ending address is specified, only one LU (identified by the <i>lu-start</i> argument) will be defined in the pool.
<b>inactivity-timeout</b> <i>minutes</i>	(Optional) Interval of inactivity (in minutes) on either the SSCP-LU or LU-LU sessions, which will cause the downstream LU to be disconnected from the upstream LU. The default is disabled.

## dspu pu (Frame Relay)

To define a DSPU host over a Frame Relay connection, use the **dspu pu** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu pu pu-name dlci dlci-number [rsap remote-sap] [lsap local-sap] [xid-rcv xid]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout]
```

```
no dspu pu pu-name dlci dlci-number [rsap remote-sap] [lsap local-sap] [xid-rcv xid]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout]
```

Syntax Description	
<i>pu-name</i>	Name of the downstream PU.
<b>dlci</b> <i>dlci-number</i>	Frame Relay data-link connection identifier (DLCI) number. This number is a decimal.
<b>rsap</b> <i>remote-sap</i>	(Optional) SAP address of the downstream PU. The default is 4.
<b>lsap</b> <i>local-sap</i>	(Optional) Local SAP address used by the DSPU to establish connection with the downstream PU. The default is 8.
<b>xid-rcv</b> <i>xid</i>	(Optional) Specifies a match on XID.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive sizes used for the downstream PU link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Maximum I-frame that can be sent or received across the link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is 1 to 600 seconds. The default is 30 seconds.

## dspu pu (QLLC)

To explicitly define a downstream PU over an X.25 connection, use the **dspu pu** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu pu pu-name x25 remote-x121-addr [qllc local-x121-subaddr] [xid-rcv xid]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout]
```

```
no dspu pu pu-name x25 remote-x121-addr [qllc local-x121-subaddr] [xid-rcv xid]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout]
```

## Syntax Description

<i>pu-name</i>	Name of the downstream PU.
<b>x25</b> <i>remote-x121-addr</i>	Variable-length X.121 address. It is assigned by the X.25 network service provider.
<b>qllc</b> <i>local-x121-subaddr</i>	(Optional) Local X.121 subaddress.
<b>xid-rcv</b> <i>xid</i>	(Optional) Specifies a match on XID.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive sizes used for the downstream PU link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Maximum I-frame that can be sent or received across the link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is 1 to 600 seconds. The default is 30 seconds.

## dspu pu (SDLC)

To define a DSPU host over an SDLC connection, use the **dspu pu** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu pu pu-name sdlc sdlc-addr [xid-rcv xid] [interface slot/port] [window window-size]
[maxiframe max-iframe] [retries retry-count] [retry-timeout retry-timeout]
```

```
no dspu pu pu-name sdlc sdlc-addr [xid-rcv xid] [interface slot/port] [window window-size]
[maxiframe max-iframe] [retries retry-count] [retry-timeout retry-timeout]
```

## Syntax Description

<i>pu-name</i>	Name of the downstream PU.
<b>sdlc</b> <i>sdlc-addr</i>	SDLC address.
<b>xid-rcv</b> <i>xid</i>	(Optional) Specifies a match on XID.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive sizes used for the downstream PU link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Maximum I-frame that can be sent or received across the link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is 1 to 600 seconds. The default is 30 seconds.

# dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)

To define an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, virtual data-link control, or NCIA connections, use the **dspu pu** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu pu pu-name [rmac remote-mac] [rsap remote-sap] [lsap local-sap] [xid-rcv xid]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout]
```

```
no dspu pu pu-name [rmac remote-mac] [rsap remote-sap] [lsap local-sap] [xid-rcv xid]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout]
```

## Syntax Description

<i>pu-name</i>	Name of the downstream PU.
<b>rmac</b> <i>remote-mac</i>	(Optional) MAC address of the downstream PU.
<b>rsap</b> <i>remote-sap</i>	(Optional) SAP address of the downstream PU. The default is 4.
<b>lsap</b> <i>local-sap</i>	(Optional) Local SAP address used by the DSPU to establish connection with the downstream PU. The default is 8.
<b>xid-rcv</b> <i>xid</i>	(Optional) Specifies a match on XID.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive sizes used for the downstream PU link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Maximum I-frame that can be sent or received across the link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is 1 to 600 seconds. The default is 30 seconds.

# dspu rsrb

To define the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB, use the **dspu rsrb** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu rsrb local-virtual-ring bridge-number target-virtual-ring virtual-macaddr
```

```
no dspu rsrb local-virtual-ring bridge-number target-virtual-ring virtual-macaddr
```

## Syntax Description

<i>local-virtual-ring</i>	DSPU local virtual ring number.
<i>bridge-number</i>	Bridge number connecting the DSPU local virtual ring and the RSRB target virtual ring. The valid range is 1 to 15.

<i>target-virtual-ring</i>	RSRB target virtual ring number. The RSRB target virtual ring corresponds to the ring-number parameter defined by a <b>source-bridge ring-group</b> command.
<i>virtual-macaddr</i>	DSPU virtual MAC address.

## dspu rsrb enable-host

To enable an RSRB SAP for use by DSPU host connections, use the **dspu rsrb enable-host** global configuration command. To disable the RSRB SAP, use the **no** form of this command.

```
dspu rsrb enable-host [lsap local-sap]
```

```
no dspu rsrb enable-host [lsap local-sap]
```

<b>Syntax Description</b>	<b>lsap local-sap</b> (Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connections attempts and for starting outgoing connection attempts. The default is 12.
---------------------------	---

## dspu rsrb enable-pu

To enable an RSRB SAP for use by DSPU downstream connections, use the **dspu rsrb enable-pu** global configuration command. To disable the SAP, use the **no** form of this command.

```
dspu rsrb enable-pu [lsap local-sap]
```

```
no dspu rsrb enable-pu [lsap local-sap]
```

<b>Syntax Description</b>	<b>lsap local-sap</b> (Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts.
---------------------------	---

## dspu rsrb start

To specify that an attempt will be made to connect to the remote resource defined by host name or PU name through the RSRB, use the **dspu rsrb start** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu rsrb start {host-name | pu-name}
```

```
no dspu rsrb start {host-name | pu-name}
```

<b>Syntax Description</b>	<i>host-name</i>	Name of a host defined in a <b>dspu host</b> (Token Ring, Ethernet, FDDI, RSRB, VDLC) command.
	<i>pu-name</i>	Name of a PU defined in a <b>dspu host</b> (Token Ring, Ethernet, FDDI, RSRB, VDLC) command.

## dspu start

To specify that an attempt will be made to connect to the remote resource defined by host name or PU name, use the **dspu start** interface configuration command. To cancel the definition, use the **no** form of this command.

```
dspu start {host-name | pu-name}
```

```
no dspu start {host-name | pu-name}
```

<b>Syntax Description</b>	<i>host-name</i>	Name of a host defined in a <b>dspu host</b> command.
	<i>pu-name</i>	Name of a PU defined in a <b>dspu pu</b> command.

## dspu vdlc

To identify the local virtual ring and virtual MAC address that will be used to establish DSPU host and downstream connections over DLSw+ using virtual data-link control, use the **dspu vdlc** global configuration command. To cancel the definition, use the **no** form of this command.

```
dspu vdlc ring-group virtual-mac-address
```

```
no dspu vdlc ring-group virtual-mac-address
```

<b>Syntax Description</b>	<i>ring-group</i>	Local virtual ring number identifying the SRB ring group.
	<i>virtual-mac-address</i>	Virtual MAC address that represents the DSPU virtual data-link control.

## dspu vdlc enable-host

To enable a SAP for use by DSPU host connections, use the **dspu vdlc enable-host** global configuration command. To disable the SAP, use the **no** form of this command.

```
dspu vdlc enable-host [lsap local-sap]
```

```
no dspu vdlc enable-host [lsap local-sap]
```

<b>Syntax Description</b>	<i>lsap</i> <i>local-sap</i>	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connections attempts and for starting outgoing connection attempts. The default is 12.
---------------------------	------------------------------	---

## dspu vdlc enable-pu

To enable a SAP for use by DSPU virtual data-link control downstream connections, use the **dspu vdlc enable-pu** global configuration command. To disable the SAP, use the **no** form of this command.

**dspu vdlc enable-pu** [*lsap local-sap*]

**no dspu vdlc enable-pu** [*lsap local-sap*]

<b>Syntax Description</b>	<b>lsap</b> <i>local-sap</i>	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 8.
---------------------------	------------------------------	---

## dspu vdlc start

To specify that an attempt will be made to connect to the remote resource defined by host name or PU name through virtual data-link control, use the **dspu vdlc start** global configuration command. To cancel the definition, use the **no** form of this command.

**dspu vdlc start** {*host-name* | *pu-name*}

**no dspu vdlc start** {*host-name* | *pu-name*}

<b>Syntax Description</b>	<i>host-name</i>	Name of a host defined in a <b>dspu host</b> command.
	<i>pu-name</i>	Name of a PU defined in a <b>dspu host</b> command.

## lan-name

To specify a name for the LAN that is attached to the interface, use the **lan-name** interface configuration command. This name is included in any Alert sent to the SNA host when a problem occurs on this interface or LAN. To revert to the default name, use the **no** form of this command.

**lan-name** *lan-name*

**no lan-name** *lan-name*

<b>Syntax Description</b>	<i>lan-name</i>	Name used to identify the LAN when you send Alerts to the SNA host. The default LAN name is the name of the interface.
---------------------------	-----------------	--

## show dspu

To display the status of the DSPU feature, use the **show dspu** privileged EXEC command.

**show dspu** [*pool pool-name* | [*pu* {*host-name* | *pu-name*}] [*all*]]

Syntax Description		
<b>pool</b> <i>pool-name</i>	(Optional) Name of a pool of LUs (as defined by the <b>dspu pool</b> command).	
<b>pu</b>	(Optional) Name of defined PU (as defined by either the <b>dspu pu</b> or the <b>dspu host</b> command).	
<i>host-name</i>	Name of a host defined in a <b>dspu host</b> command.	
<i>pu-name</i>	Name of a PU defined in a <b>dspu pu</b> command.	
<b>all</b>	(Optional) Displays a detailed status.	

## show sna

To display the status of the SNA Service Point feature, use the **show sna** privileged EXEC command.

```
show sna [pu host-name [all]]
```

Syntax Description		
<b>pu</b>	(Optional) Name of a host defined in an <b>sna host</b> command.	
<i>host-name</i>	(Optional) Name of a host defined in an <b>sna host</b> command.	
<b>all</b>	(Optional) Displays detailed status.	

## sna enable-host (QLLC)

To enable an X.121 subaddress for use by the SNA Service Point feature on the interface, use the **sna enable-host** interface configuration command. To disable SNA Service Point on the interface, use the **no** form of this command.

```
sna enable-host qlc x121-subaddress
```

```
no sna enable-host qlc x121-subaddress
```

Syntax Description		
<b>qlc</b>	Required keyword for QLLC data-link control.	
<i>x121-subaddress</i>	X.121 subaddress.	

## sna enable-host (SDLC)

To enable an SDLC address for use by host connections, use the **sna enable-host** interface configuration command. To cancel the definition, use the **no** form of this command.

```
sna enable-host sdlc sdlc-address
```

```
no sna enable-host sdlc sdlc-address
```

Syntax Description		
<b>sdlc</b>	Required keyword for SDLC data-link control.	
<i>sdlc-address</i>	SDLC address.	

## sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)

To enable SNA on the interface, use the **sna enable-host** interface configuration command. To disable SNA on the interface, use the **no** form of this command.

**sna enable-host** [*lsap lsap-address*]

**no sna enable-host** [*lsap lsap-address*]

<b>Syntax Description</b>	<b>lsap</b>	(Optional) Activate a local SAP as an upstream SAP, for both receiving ConnectIn attempts and for starting ConnectOut attempts.
	<i>lsap-address</i>	(Optional) Local SAP. The default is 12.

## sna host (Frame Relay)

To define a link to an SNA host over a Frame Relay connection, use this form of the **sna host** global configuration command. To cancel the definition, use the **no** form of this command.

**sna host** *host-name* **xid-snd** *xid* **dldci** *dldci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*]  
 [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*]  
 [**retry-timeout** *retry-timeout*] [**focalpoint**]

**no sna host** *host-name* **xid-snd** *xid* **dldci** *dldci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*]  
 [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*]  
 [**retry-timeout** *retry-timeout*] [**focalpoint**]

<b>Syntax Description</b>	<i>host-name</i>	Specified SNA host.
	<b>xid-snd</b> <i>xid</i>	XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
	<b>dldci</b> <i>dldci-number</i>	DLCI number.
	<b>rsap</b> <i>remote-sap</i>	(Optional) SAP address of the remote host PU. The default is 4.
	<b>lsap</b> <i>local-sap</i>	(Optional) Local SAP address used by the SNA Service Point to establish connection with the remote host. The default is 12.
	<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
	<b>window</b> <i>window-size</i>	(Optional) Send and receive window sizes used for the host link. The range is 1 to 127. The default is 7.
	<b>maxiframe</b> <i>max-iframe</i>	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
	<b>retries</b> <i>retry-count</i>	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.

<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>	(Optional) Host link to be used for the focal point support.

## sna host (QLLC)

To define a link to an SNA host over an X.25/QLLC connection, use this form of the **sna host** global configuration command. To cancel the definition, use the **no** form of this command.

```
sna host host-name xid-snd xid x25 remote-x121-addr [qllc local-x121-subaddr]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

```
no sna host host-name xid-snd xid x25 remote-x121-addr [qllc local-x121-subaddr]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

Syntax Description	
<i>host-name</i>	SNA host.
<b>xid-snd</b> <i>xid</i>	XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
<b>x25</b> <i>remote-x121-addr</i>	SDLC address.
<b>qllc</b> <i>local-x121-subaddr</i>	(Optional) Specifies the SAP address of the remote host PU. The default is 4.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive window sizes used for the host link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>	(Optional) Host link to be used for the focal point support.

## sna host (SDLC)

To define a link to an SNA host over an SDLC connection, use this form of the **sna host** global configuration command. To cancel the definition, use the **no** form of this command.

```
sna host host-name xid-snd xid sdlc sdlc-addr [rsap remote-sap] [lsap local-sap]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

```
no sna host host-name xid-snd xid rmac remote-mac [rsap remote-sap] [lsap local-sap]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

Syntax Description		
<i>host-name</i>		SNA host.
<b>xid-snd</b> <i>xid</i>		XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
<b>sdlc</b> <i>sdlc-addr</i>		SDLC address.
<b>rsap</b> <i>remote-sap</i>		(Optional) SAP address of the remote host PU. The default is 4.
<b>lsap</b> <i>local-sap</i>		(Optional) Local SAP address used by the SNA Service Point to establish connection with the remote host. The default is 12.
<b>interface</b> <i>slot/port</i>		(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>		(Optional) Send and receive window sizes used for the host link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>		(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>		(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
<b>retry-timeout</b> <i>retry-timeout</i>		(Optional) Delay (in seconds) between attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>		(Optional) Host link to be used for the focal point support.

# sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)

To define a link to an SNA host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control connections, use the **sna host** global configuration command. To cancel the definition, use the **no** form of this command.

```
sna host host-name xid-snd xid rmac remote-mac [rsap remote-sap] [lsap local-sap]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

```
no sna host host-name xid-snd xid rmac remote-mac [rsap remote-sap] [lsap local-sap]
[interface slot/port] [window window-size] [maxiframe max-iframe] [retries retry-count]
[retry-timeout retry-timeout] [focalpoint]
```

## Syntax Description

<i>host-name</i>	SNA host.
<b>xid-snd</b> <i>xid</i>	XID that will be sent to the host during connection establishment. The XID value is 8 hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
<b>rmac</b> <i>remote-mac</i>	MAC address of the remote host PU.
<b>rsap</b> <i>remote-sap</i>	(Optional) SAP address of the remote host PU. The default is 4.
<b>lsap</b> <i>local-sap</i>	(Optional) Local SAP address used by the SNA Service Point to establish connection with the remote host. The default is 12.
<b>interface</b> <i>slot/port</i>	(Optional) Slot and port number of the interface.
<b>window</b> <i>window-size</i>	(Optional) Send and receive window sizes used for the host link. The range is 1 to 127. The default is 7.
<b>maxiframe</b> <i>max-iframe</i>	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 64 to 18432. The default is 1472.
<b>retries</b> <i>retry-count</i>	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
<b>retry-timeout</b> <i>retry-timeout</i>	(Optional) Delay (in seconds) between attempts to retry establishing connection with remote host PU. The range is 1 to 600 seconds. The default is 30 seconds.
<b>focalpoint</b>	(Optional) Host link to be used for the focal point support.

## sna rsrb

To specify the entities that the SNA feature will simulate at the remote source-route bridge (RSRB), use the **sna rsrb** interface configuration command. To cancel the specification, use the **no** form of this command.

```
sna rsrb local-virtual-ring bridge-number target-virtual-ring virtual-macaddr
```

```
no sna rsrb local-virtual-ring bridge-number target-virtual-ring virtual-macaddr
```

Syntax Description		
	<i>local-virtual-ring</i>	Local virtual ring number.
	<i>bridge-number</i>	Virtual bridge number. The valid range is 1 to 15.
	<i>target-virtual-ring</i>	Target virtual ring number.
	<i>virtual-macaddr</i>	Virtual MAC address.

## sna rsrb enable-host

To enable an RSRB SAP for use by SNA Service Point feature, use the **sna rsrb enable-host** global configuration command. To disable the RSRB SAP, use the **no** form of this command.

**sna rsrb enable-host** [**lsap** *local-sap*]

**no sna rsrb enable-host** [**lsap** *local-sap*]

Syntax Description		
	<b>lsap</b> <i>local-sap</i>	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connections attempts and for starting outgoing connection attempts. The default is 12.

## sna rsrb start

To specify that an attempt will be made to connect to the remote resource defined by host name through the RSRB, use the **sna rsrb start** global configuration command. To cancel the definition, use the **no** form of this command.

**sna rsrb start** *host-name*

**no sna rsrb start** *host-name*

Syntax Description		
	<i>host-name</i>	The name of a host defined in an <b>sna host</b> or equivalent command.

## sna start

To initiate a connection to a remote resource, use the **sna start** interface configuration command. To cancel the connection attempt, use the **no** form of this command.

**sna start** [*resource-name*]

**no sna start** [*resource-name*]

Syntax Description		
	<i>resource-name</i>	(Optional) Name of a host defined in an <b>sna host</b> command.

## sna vdlc

To identify the local virtual ring and virtual MAC address that will be used to establish SNA host connections over DLSw+ using virtual data-link control, use the **sna vdlc** global configuration command. To cancel the definition, use the **no** form of this command.

**sna vdlc** *ring-group virtual-mac-address*

**no sna vdlc** *ring-group virtual-mac-address*

Syntax Description		
	<i>ring-group</i>	Local virtual ring number identifying the SRB ring group.
	<i>virtual-mac-address</i>	Virtual MAC address that represents the SNA virtual data-link control.

## sna vdlc enable-host

To enable a SAP for use by SNA Service Point feature, use the **sna vdlc enable-host** global configuration command. To disable the SAP, use the **no** form of this command.

**sna vdlc enable-host** [**lsap** *local-sap*]

**no sna vdlc enable-host** [**lsap** *local-sap*]

Syntax Description		
	<b>lsap</b> <i>local-sap</i>	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 12.

## sna vdlc start

To specify that an attempt will be made to connect to the remote resource defined by host name through virtual data-link control (VDLC), use the **sna vdlc start** global configuration command. To cancel the definition, use the **no** form of this command.

**sna vdlc start** *host-name*

**no sna vdlc start** *host-name*

Syntax Description		
	<i>host-name</i>	The name of a host defined in an <b>sna host</b> or equivalent command.





## SNA Switching Services Commands

This chapter describes the function and syntax of the SNA Switching Services (SNASw) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*.

### ping sna

To initiate an APPC session with a named destination LU to run the APING transaction program to check network integrity and timing characteristics, use the **ping sna** privileged EXEC command.

```
ping sna [-1] [-c consecutive packets] [-i number-iterations] [-m mode] [-n] [-r] [-s size]
          [-t tpname] [-u userid -p password] destination
```

#### Syntax Description

<b>-1</b>	(Optional) Sends data from client to server only (no echo).
<b>-c</b> <i>consecutive blocks</i>	(Optional) Specifies the number of data blocks sent per iteration.
<b>-i</b> <i>number-iterations</i>	(Optional) Specifies number of iterations.
<b>-m</b> <i>mode</i>	(Optional) Specifies APPC mode to use.
<b>-n</b>	(Optional) Skips any security (SECURITY=NONE).
<b>-r</b>	(Optional) Displays route taken by APPC PING.
<b>-s</b> <i>size</i>	(Optional) Specifies the size of the of the data block to be sent.
<b>-t</b> <i>tpname</i>	(Optional) Specifies TP to start on the server.
<b>-u</b> <i>userid</i>	(Optional) Specifies USERID.
<b>-p</b> <i>password</i>	(Optional) Specifies the password associated with the userid specified after <b>-u</b> . Required when <b>-u</b> is specified. Password must be 1 to 8 characters.
<i>destination</i>	Specifies the fully qualified name of the destination logical unit or control point with which an APING transaction should be initiated.

### show snasw class-of-service

To display the COS definitions predefined to SNASw, use the **show snasw class-of-service** command.

```
show snasw class-of-service [brief | detail]
```

<b>Syntax Description</b>	<b>brief</b>	(Optional) Indicates a one-line display per displayed resource. The brief version displays COS name, transmission priority, and number of node and TG rows.
	<b>detail</b>	(Optional) Indicates a detailed, multiline display of all fields returned for COS display.

## show snasw connection-network

To display the connection networks (virtual nodes) defined to the local node, use the **show snasw connection-network** command.

```
show snasw connection-network [brief | detail]
```

<b>Syntax Description</b>	<b>brief</b>	(Optional) Indicates a one-line display per resource. The brief version displays the connection network name, the number of attached ports, and the port names in the connection network.
	<b>detail</b>	(Optional) Indicates a detailed, multiline display of all fields returned for connection-network display.

## show snasw directory

To display the SNASw directory entries, use the **show snasw directory** command.

```
show snasw directory [name resourcenamefilter] [brief | detail ]
```

<b>Syntax Description</b>	<b>name resourcenamefilter</b>	(Optional) Indicates the fully qualified name of the resource (1 to 17 characters). Only resource names that match the specified name are displayed.
	<b>brief</b>	(Optional) Indicates a one-line display for each resource. The brief version displays resource name, owning CP name, network node server name, and entry type.
	<b>detail</b>	(Optional) Indicates a detailed, multiline display of all fields returned for the directory display.

## show snasw dlctrace

To display the captured DLC trace information to the console, use the **show snasw dlctrace** command.

```
show snasw dlctrace [all | last number-records | next number-records] [brief | detail]
[filter filter-string] [id recordid]
```

Syntax Description		
<b>all</b>		(Optional) Indicates that all records in the dlctrace buffer are displayed.
<b>last</b> <i>number-records</i>		(Optional) Indicates the last <i>n</i> frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
<b>next</b> <i>number-records</i>		(Optional) Indicates the next frames after the record identified in the ID operand (or from the beginning of the trace if the ID operand is not coded) are displayed.
<b>brief</b>		(Optional) Indicates a one-line display per trace entry describing the type of frame traced.
<b>detail</b>		(Optional) Indicates a a detailed, multiline display of the frame that displays the brief information plus a hexadecimal dump of the entire frame.
<b>filter</b> <i>filter-string</i>		(Optional) Indicates that a string follows against which the formatted trace output are filtered. Only frames that contain the filter-string are displayed.
<b>id</b> <i>recordid</i>		(Optional) Indicates the 1 to 999,999 trace record identifier. Only the frame ID that matches the record specified is displayed.

## show snasw dlus

To display the SNASw DLUS objects, use the **show snasw dlus** command.

```
show snasw dlus [brief | detail]
```

Syntax Description		
<b>brief</b>		(Optional) Indicates that one line per DLUS is displayed. The brief version includes the DLUS name, state (active or inactive), port name, cpname, node type, and number of active PUs on the DLUS.
<b>detail</b>		(Optional) Indicates the detailed, multiline display that shows all fields returned for DLUS displayed.

## show snasw ipstrace

To display the interprocess signal trace on the router console, use the **show snasw ipstrace** command.

```
show snasw ipstrace [all | next number-records | last number-records] [filter filter-string]
[id recordid]
```

Syntax Description		
<b>all</b>		(Optional) Specifies all records are displayed
<b>next</b> <i>number-records</i>		(Optional) Displays records from beginning or following record IS.
<b>last</b> <i>number-records</i>		(Optional) Indicates that the last <i>n</i> frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
<b>filter</b> <i>filter-string</i>		(Optional) Indicates that a string follows against which the formatted trace output is filtered. Only frames that contain the filter-string are displayed.
<b>id</b> <i>recordid</i>		(Optional) Indicates the 1 to 999,999 trace record identifier. Only the frame ID that matches the record specified are displayed.

## show snasw link

To display the SNASw link objects, use the **show snasw link** command.

```
show snasw link [brief | detail] [cpname cpnamefilter] [name linknamefilter]
[port portnamefilter] [rmac macfilter] [xid xidfilter]
```

Syntax Description		
<b>brief</b>	(Optional) Indicates that one line per link is displayed. The brief version includes the link name, state (active or inactive), port name, adjacent CP name, node type information, number of sessions, and HPR support. The number of sessions does not include HPR sessions.	
<b>detail</b>	(Optional) Indicates that a detailed, multiline display that shows all fields returned for links displayed.	
<b>cpname</b> <i>cpnamefilter</i>	(Optional) Indicates a fully qualified cpname (1 to 17 characters). Only links with CP names (as known to the router) that match the specified cpname are displayed.	
<b>name</b> <i>linknamefilter</i>	(Optional) Indicates the name of the link to be displayed. Only links matching this name are displayed.	
<b>port</b> <i>portnamefilter</i>	(Optional) Indicates the handle “naming” for the specific port (1 to 8 characters). All links associated with a port matching the filter are displayed.	
<b>rmac</b> <i>macfilter</i>	(Optional) Indicates a 48-bit MAC address in hexadecimal form. Only links with a remote MAC address matching the MAC address specified are displayed.	
<b>xid</b> <i>xidfilter</i>	(Optional) Indicates a 4-byte XID (idnum/idblk) specified in hexadecimal form. Only links matching the configured XID are displayed.	

## show snasw lu

To display the SNASw dependent LUs, use the **show snasw lu** command.

```
show snasw lu [brief | detail] [name luname] [pu puname]
```

Syntax Description		
<b>brief</b>	(Optional) Indicates that one line per LU is displayed. The brief display includes LU name, PU name, DLUS name, and PLU name.	
<b>detail</b>	(Optional) Indicates that a detailed, multiline display that shows all possible fields returned for the link is displayed.	
<b>name</b> <i>luname</i>	(Optional) Indicates an LU name to filter. Only LUs matching the specified name are displayed.	
<b>pu</b> <i>puname</i>	(Optional) Indicates a PU name to filter. Only LUs for the specified name PU are displayed.	

## show snasw mode

To display the SNASw modes, use the **show snasw mode** command.

```
show snasw mode
```

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

## show snasw node

To display details and statistics of the SNASw operation, use the **show snasw node** command.

```
show snasw node
```

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

## show snasw pdlog

To display entries in the cyclical problem determination log to the console, use the **show snasw pdlog** command.

```
show snasw pdlog [brief | detail] [all | next number-records | last number-records]
[filter filterstring] [id recordid]
```

Syntax Description		
<b>brief</b>	(Optional)	Indicates that a one-line description for each pdlog entry is returned.
<b>detail</b>	(Optional)	Indicates that a multiline display is returned.
<b>all</b>	(Optional)	Specifies all records are displayed.
<b>next number-records</b>	(Optional)	Displays records from the beginning or following a record ID.
<b>last number-records</b>	(Optional)	Indicates that the last <i>n</i> frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
<b>filter filterstring</b>	(Optional)	Shows output filtered on a specific string.
<b>id recordid</b>	(Optional)	Indicates the 1 to 99999 trace record identifier. Only the frame ID that matches the record specified is displayed.

## show snasw port

To display the SNASw port objects, use the **show snasw port** command.

```
show snasw port [brief | detail] [name portnamefilter]
```

Syntax Description		
<b>brief</b>	(Optional)	Indicates that a one-line description for each port entry is displayed.
<b>detail</b>	(Optional)	Indicates that a multiline display is returned.
<b>name</b> <i>portnamefilter</i>	(Optional)	Indicates the name of the port to filter for which information is displayed. Only ports matching name are displayed.

## show snasw pu

To display the SNASw PUs that require or request SSCP-PU services, use the **show snasw pu** command.

```
show snasw pu [brief | detail] [dlus dlusfilter] [name punamefilter]
```

Syntax Description		
<b>brief</b>	(Optional)	Indicates that one-line per PU is displayed. The brief version includes the PU name, PU ID, state, defined DLUS, and current DLUS.
<b>detail</b>	(Optional)	Indicates that a detailed, multiline display that shows all possible fields returned for a link is displayed.
<b>dlus</b> <i>dlusfilter</i>	(Optional)	Indicates the fully qualified DLUS name (1 to 17 characters). Only PUs that are currently served by the DLUS specified are displayed.
<b>name</b> <i>punamefilter</i>	(Optional)	Indicates a PU name to filter (1 to 8 characters). Only PUs matching this name are displayed.

## show snasw rtp

To display the SNASw RTP connections, use the **show snasw rtp** command.

```
show snasw rtp [brief | detail] [class-of-service cosname] [cpname netid.cpname] [name connectionnamefilter] [tcid tcidconnection]
```

Syntax Description		
<b>brief</b>	(Optional)	Indicates that one-line per RTP is displayed. The brief version includes the RTP name, local TCID, remote TCID, remote cpname, and COS.
<b>detail</b>	(Optional)	Indicates a detailed, multiline display with all fields returned for RTP is displayed.
<b>class-of-service</b> <i>cosname</i>	(Optional)	Shows specific HPR RTP connections by COS name.
<b>cpname</b> <i>netid.cpname</i>	(Optional)	Shows specific HPR RTP connections by fully qualified partner CP name, consisting of both network ID and cpname.
<b>name</b> <i>connectionnamefilter</i>	(Optional)	Indicates the name of the RTP connection (1 to 8 characters). Only TG records origins or destinations that match the specified name or node records are displayed.
<b>tcid</b> <i>tcidconnection</i>	(Optional)	Shows the specific HPR RTP connection for the local TCID connections.

## show snasw session

To display the SNASw session objects, use the **show snasw session** command.

```
show snasw session [local | dlur | intermediate] [name sessionnamefilter] [pcid pcidfilter]
[brief | detail | intermediate]
```

Syntax Description		
	<b>local</b>	(Optional) Indicates that the scope of the display is limited to the types of sessions indicated. Local sessions are those that terminate on the node. Examples include CP-CP sessions and DLUR-DLUS sessions.
	<b>dlur</b>	(Optional) Indicates that the scope of the display is limited to the types of sessions indicated. DLUS sessions are LU-LU sessions passing through the node, which are using the DLUR for dependent session.
	<b>intermediate</b>	(Optional) Indicates that the scope of the display is limited to the types of sessions indicated. Intermediate sessions are LU-LU sessions passing through the node and are not DLUR-associated.
	<b>name sessionnamefilter</b>	(Optional) Indicates the fully qualified name (1 to 17 characters). Only sessions that have a local or remote endpoint LU name matching the supplied name are displayed.
	<b>pcid pcidfilter</b>	(Optional) Indicates an 8-byte PCID specified in hexadecimal form. All sessions matching the PCID filter are displayed.
	<b>brief</b>	(Optional) Indicates that one-line per session is displayed. The brief version includes PCID, state (active or inactive), session endpoint LU names, and mode.
	<b>detail</b>	(Optional) Indicates a detailed, multiline display that shows all fields returned for the session is displayed.

## show snasw statistics

To display the SNASw node-wide information, use the **show snasw statistics** command.

```
show snasw statistics
```

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

## show snasw summary-ipstrace

To display the continuously running “footprint” summary interprocess signal trace on the router console, use the **show snasw summary-ipstrace** command.

```
show snasw summary-ipstrace [all | next number-records | last number-records] [id recordid ]
[filter filter-string]
```

Syntax Description		
<b>all</b>		(Optional) Specifies all records are displayed.
<b>next</b> <i>number-records</i>		(Optional) Displays records from the start or starting with the record ID.
<b>last</b> <i>number-records</i>		(Optional) Displays records from the end or prior to the record ID. Indicates that the last <i>n</i> frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
<b>id</b> <i>recordid</i>		(Optional) Indicates a 1 to 999,999 trace record identifier.
<b>filter</b> <i>filter-string</i>		(Optional) Indicates that a string follows against which the formatted trace output is filtered. Only frames that contain the <i>filter-string</i> are displayed.

## show snasw topology

To display the SNASw topology records, use the **show snasw topology** command.

```
show snasw topology [name cnamefilter] [brief | detail]
```

Syntax Description		
<b>name</b> <i>cnamefilter</i>		(Optional) Indicates the fully qualified name of the CP (1 to 17 characters). Only records that match the <i>cname</i> specified are displayed.
<b>brief</b>		(Optional) Indicates one line per topology record is displayed.
<b>detail</b>		(Optional) Indicates a detailed, multiline display of topology information.

## snasw cname

To define a control point name for SNASw, use the **snasw cname** global configuration command. To deactivate SNASw and remove the control point definition, use the **no** form of this command.

```
snasw cname {netid.cname | netid [hostname] ip-address interface-name}
```

```
no snasw cname
```

Syntax Description		
<i>netid.cname</i>		Fully qualified CP name for this node, consisting of both network ID and <i>cname</i> .
<i>netid</i>		Partial CP name, which consists of only a network ID. If this option is selected, the <i>hostname</i> or <i>IP address</i> operands must also be configured to complete the fully qualified <i>cname</i> .
<i>hostname</i>		(Optional) Indicates a CP name built using the <i>hostname</i> configured on the router. When configuring this operand, code a NET ID only. The last eight characters of the <i>hostname</i> are used to complete the CP name.

<b>ip-address</b> <i>interface-name</i>	(Optional) Indicates the CP name built by deriving the cpname from the IP address on the interface indicated in the <i>interface-name</i> . When configured, this operand requires a <i>netid</i> operand. In addition, a portion of the cpname may be configured. The remaining characters of the cpname that are not configured are generated from the IP address indicated.  The generated characters are derived from a hexadecimal format of the IP address for the interface specified.
---	---

## snasw dlcfiler

To filter frames being captured, use the **snasw dlcfiler** global configuration command. To disable the filtering of frames arriving and leaving SNASw, use the **no** form of this command.

```
snasw dlcfiler [link linkname [session session-address]] [port portname] [rmac
mac-address-value [session session-address]] [rtp rtp-name [session session-address]]
[type [cls] [hpr-cntl] [hpr-data] [isr] [xid]
```

```
no snasw dlcfiler
```

Syntax Description	
<b>link</b> <i>linkname</i> [ <b>session</b> <i>session-address</i> ]	(Optional) Specifies the link name upon which the DLC trace is filtered (one to eight characters). All incoming and outgoing frames matching this link are traced.
<b>port</b> <i>portname</i>	(Optional) Specifies the port name upon which the port is filtered (one to eight characters). All incoming and outgoing frames matching this port are traced.
<b>rmac</b> <i>mac-address-value</i> [ <b>session</b> <i>session-address</i> ]	(Optional) Specifies the MAC address upon which the DLC trace is filtered. All incoming and outgoing frames matching this MAC address are traced.
<b>rtp</b> <i>rtp-name</i> [ <b>session</b> <i>session-address</i> ]	(Optional) Specifies the RTP name upon which the RTP is filtered (one to eight characters). All incoming and outgoing frames matching this RTP connection name are traced.
<b>type</b>	(Optional) Indicates that one or more frame type filters follow. Use the <b>type</b> operand to further refine the filter to specify one or more frame types.
<b>cls</b>	(Optional) Indicates that commands to the local DLC are traced.
<b>hpr-cntl</b>	(Optional) Indicates that the HPR format identifier 5 (FID5), which does not carry an SNA data payload, is traced.
<b>hpr-data</b>	(Optional) Indicates that the HPR format identifier 5 (FID5), which carry an SNA data payload, is traced.
<b>isr</b>	(Optional) Indicates that the SNA and APPN format identifier 2 (FID2) are traced.
<b>xid</b>	(Optional) Indicates that the XID frames are traced.

## snasw dlctrace

To trace frames arriving and leaving SNASw, use the **snasw dlctrace** global configuration command. To deactivate the capture of frame data and free the storage buffer used to capture the data, use the **no** form of this command.

```
snasw dlctrace [buffer-size buffer-size-value] [file filename [timestamp]] [frame-size
frame-size-value | auto-terse] [format [brief | detail | analyzer]] [nostart]
```

```
no snasw dlctrace
```

### Syntax Description

<b>buffer-size</b> <i>buffer-size-value</i>	(Optional) Specifies the size (in kilobytes) of the DLC trace buffer requested. The minimum buffer size is 100, while the maximum is 16000.
<b>file</b> <i>filename</i>	(Optional) Specifies the file name for the DLC trace buffer file when writing this file to the file server. Use the following format: protocol://host/path/filename.
<b>timestamp</b>	(Optional) Appends the current date and time to the end of the file when it is dumped.
<b>frame-size</b> <i>frame-size-value</i>	(Optional) Indicates the size of the frame that is traced within the DLC trace. All data beyond the size value are truncated and are not included in the trace. The default is that the entire frame is traced.
<b>auto-terse</b>	(Optional) Indicates LU-LU and SSCP-LU session data frames should be truncated after the SNA RH. Also truncates NMVTs on the SSCP-PU session. Control frames (for example, XID, BIND, ACTPU) are traced in their entirety.
<b>format</b>	(Optional) Indicates the format the DLC trace is written to when writing to a file server. Valid values are <b>brief</b> , <b>detail</b> , and <b>analyzer</b> : <ul style="list-style-type: none"> <li><b>brief</b>—Indicates a text file is written with a one-line-per-frame summary for each frame.</li> <li><b>detail</b>—Indicates a text file is written with a frame summary line followed by a complete hexadecimal dump of the frame.</li> <li><b>analyzer</b>—Indicates a binary file is generated that is readable by several popular network analyzer products. This format uses the Network Associates Sniffer file format.</li> </ul>
<b>nostart</b>	(Optional) Indicates that the specified trace is not to be started when the subsystem is started.

## snasw dlus

To specify parameters related to DLUR/DLUS functionality, use the **snasw dlus** global configuration command. To remove the data specified in a previous **snasw dlus** command, use the **no** form of this command.

```
snasw dlus primary-dlus-name [backup backup-dlus-name] [prefer-active] [retry interval count]
```

```
no snasw dlus
```

Syntax Description		
	<i>primary-dlus-name</i>	Specifies the fully qualified name of the primary DLUS (3 to 17 characters).
	<b>backup</b> <i>backup-dlus-name</i>	(Optional) Indicates configuration of a backup DLUS. A backup DLUS is used when the primary DLUS is unreachable or cannot service a specific downstream device. The fully qualified name of the backup DLUS is 3 to 17 characters in length.
	<b>prefer-active</b>	(Optional) Indicates that if an active DLUS/DLUR connection was established, an incoming PU will retry exclusively on the active DLUS connection and will not attempt to connect to a different DLUS.
	<b>retry</b> <i>interval count</i>	(Optional) Indicates that the DLUR retry parameters follow this statement. Interval indicates the time period between attempts to connect a DLUS if one is not serving a specific PU. Retry indicates the number of times the current or primary DLUS is retried before attempting to connect to a backup or currently inactive DLUS.

## snasw dump

To copy problem determination logs and traces from internal buffers to an external file server, use the **snasw dump** privileged EXEC command.

**snasw dump all | dlctrace | ipstrace | summary-ipstrace | pdlog**

Syntax Description		
	<b>all</b>	Indicates all configured trace and problem determination buffers should be transferred. The <b>file</b> operand must be configured on the enabling configuration command for the buffers to be dumped. Traces that run but do not have the <b>file</b> operand coded are not transferred.
	<b>dlctrace</b>	Indicates the DLC trace buffer is transferred to a file server. If <b>file</b> is configured on the <b>snasw dlctrace</b> command, the URL specified is used for transferring the DLC trace file. If <b>file</b> is not configured on the <b>snasw dlctrace</b> command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.
	<b>ipstrace</b>	Indicates the IPS trace buffer is transferred to a file server. If <b>file</b> is configured on the <b>snasw ipstrace</b> command, the URL specified is used for transferring the ipstrace file. If <b>file</b> is not configured on the <b>snasw ipstrace</b> command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.
	<b>summary-ipstrace</b>	Indicates the summary IPS trace buffer is transferred to a file server. If <b>file</b> is coded on the <b>snasw summary-ipstrace</b> command, the URL specified is used for transferring the summary ipstrace file. If <b>file</b> is not coded on the <b>snasw ipstrace</b> command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.
	<b>pdlog</b>	Indicates the problem determination log buffer is transferred to a file server. If <b>file</b> is coded on the <b>snasw pdlog</b> command, the URL specified is used for transferring the pdlog file. If <b>file</b> is not coded, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.

## snasw event

To indicate which normal events are logged to the console, use the **snasw event** global configuration command. To return the events to their default state, use the **no** form of this command.

```
snasw event [cpcp] [dlc] [implicit-ls] [port]
```

```
no snasw event
```

Syntax Description		
	<b>cpcp</b>	(Optional) Indicates that an event is issued for CP-CP session state changes.
	<b>dlc</b>	(Optional) Indicates DLC state changes.
	<b>implicit-ls</b>	(Optional) Indicates state change on implicit links, including connection network links.
	<b>port</b>	(Optional) Indicates that an event is issued for port state changes.

## snasw ip-precedence

To define IP type of service (TOS) precedence settings to be mapped to APPN priorities, use the **snasw ip-precedence** global configuration command. To remove the precedence settings, use the **no** form of this command.

```
snasw ip-precedence link link-setting network network-setting high high-setting medium
medium-setting low low-setting
```

```
no snasw ip-precedence link link-setting network network-setting high high-setting medium
medium-setting low low-setting
```

Syntax Description		
	<b>link</b> <i>link-setting</i>	TOS precedence setting (0-7) mapped to link control (LDLC) priority.
	<b>network</b> <i>network-setting</i>	TOS precedence setting (0-7) mapped to network priority.
	<b>high</b> <i>high-setting</i>	TOS precedence setting (0-7) mapped to high priority.
	<b>medium</b> <i>medium-setting</i>	TOS precedence setting (0-7) mapped to medium priority.
	<b>low</b> <i>low-setting</i>	TOS precedence setting (0-7) mapped to low priority.

## snasw ipsfilter

To filter interprocess signal trace elements being traced using the **snasw ipstrace** or **debug snasw ips** commands, use the **snasw ipsfilter** global configuration command. To remove all filtering, use the **no** form of this command.

```
snasw ipsfilter [as] [asm] [bm] [ch] [cpc] [cs] [di] [dlc] [dma] [dr] [ds] [es] [ha] [hpr] [hs] [lm]
[mds] [ms] [nof] [pc] [ps] [pu] [px] [rm] [rtp] [ru] [scm] [sco] [sm] [spc] [ss] [trs]
```

```
no snasw ipsfilter
```

**Syntax Description**

<b>as</b>	(Optional) Specifies a filter on the Address Space component.
<b>asm</b>	(Optional) Specifies a filter on the Address Space Manager component.
<b>bm</b>	(Optional) Specifies a filter on the Buffer Management component.
<b>ch</b>	(Optional) Specifies a filter on the Channel component.
<b>cpc</b>	(Optional) Specifies a filter on the CPI-C component.
<b>cs</b>	(Optional) Specifies a filter on the Configuration Services component.
<b>di</b>	(Optional) Specifies a filter on the Defect Indication component.
<b>dlc</b>	(Optional) Specifies a filter on the Data Link Control component.
<b>dma</b>	(Optional) Specifies a filter on the Direct Memory Access component.
<b>dr</b>	(Optional) Specifies a filter on the Dependent LU Requester component.
<b>ds</b>	(Optional) Specifies a filter on the Directory Services component.
<b>es</b>	(Optional) Specifies a filter on the End System component.
<b>ha</b>	(Optional) Specifies a filter on the High Availability component.
<b>hpr</b>	(Optional) Specifies a filter on the High-Performance Routing component.
<b>hs</b>	(Optional) Specifies a filter on the Half Session component.
<b>lm</b>	(Optional) Specifies a filter on the LU Manager component.
<b>mds</b>	(Optional) Specifies a filter on the Management Data Stream component.
<b>ms</b>	(Optional) Specifies a filter on the Management Services component.
<b>nof</b>	(Optional) Specifies a filter on the Node Operator Facility component.
<b>pc</b>	(Optional) Specifies a filter on the Path Control component.
<b>ps</b>	(Optional) Specifies a filter on the Presentation Services component.
<b>pu</b>	(Optional) Specifies a filter on the PU Manager component.
<b>px</b>	(Optional) Specifies a filter on the PU Concentration component.
<b>rm</b>	(Optional) Specifies a filter on the Resource Manager component.
<b>rtp</b>	(Optional) Specifies a filter on the Rapid Transport Protocol component.
<b>ru</b>	(Optional) Specifies a filter on the Request Unit Interface component.
<b>scm</b>	(Optional) Specifies a filter on the Session Connect Manager component.
<b>sco</b>	(Optional) Specifies a filter on the Session Connector component.
<b>sm</b>	(Optional) Specifies a filter on the Session Manager component.
<b>spc</b>	(Optional) Specifies a filter on the Serial Protocol Channel component.
<b>ss</b>	(Optional) Specifies a filter on the Session Services component.
<b>trs</b>	(Optional) Specifies a filter on the Topology Routing Services component.

## snasw ipstrace

To set up a trace buffer and begin tracing IPS trace elements, use the **snasw ipstrace** global configuration command. To turn off the capture of trace elements and to free the trace buffer, use the **no** form of this command.

```
snasw ipstrace [buffer-size buffer-size-value] [file filename timestamp]
```

```
no snasw ipstrace
```

Syntax Description		
<b>buffer-size</b> <i>buffer-size-value</i>	(Optional) Indicates that this trace command controls the size of the buffer used for storing ipstrace elements (in kilobytes). The default is 500 KB. The minimum buffer size is 10 KB; the maximum is 16000 KB.	
<b>file</b> <i>filename</i>	(Optional) Specifies the file name for the IPS trace buffer file when writing this file to the server.	
<b>timestamp</b>	(Optional) Appends the current date and time to the end of the file when it is dumped.	

## snasw link

To configure upstream links, use the **snasw link** global configuration command. To remove the configuration of upstream links, use the **no** form of this command.

```
snasw link linkname port portname rmac mac-address | ip-dest ip-address [rsap sap-value] [nns]
[tgp [high | low | medium | secure]] [nostart]
```

```
no snasw link linkname
```

Syntax Description		
<b>linkname</b> <i>linkname</i>	Indicates the one-to-eight character local name for this link. This name is used to identify the link in <b>show</b> and privileged EXEC commands.	
<b>port</b> <i>portname</i>	Specifies the SNASw port from which this link will connect.	
<b>rmac</b> <i>mac-address</i>	Specifies the 48-bit MAC address of the destination station. Either this operand or <b>ip-dest</b> is required. RMAC is required for all links associated with ports that are not HPR/IP ports.	
<b>ip-dest</b> <i>ip-address</i>	Indicates the IP address or DNS name of the destination stations. Either this operand or <b>rmac</b> is required. For all links associated with HPR/IP ports, <b>ip-dest</b> is required.	
<b>rsap</b> <i>sap-value</i>	(Optional) Indicates the destination SAP value, which defaults to 4.	
<b>nns</b>	(Optional) Configures the adjacent link as a preferred network node server.  If the primary NN server (uplink) fails, CP-CP sessions are established with a backup, if one is available. When the link to the primary recovers, SNASw retains the CP-CP sessions established with the backup and does not automatically switch back to the primary. To force SNASw to switch back to the primary, use the <b>snasw stop cp-cp</b> command. (If the link to the backup fails, SNASw does switch back to the primary automatically.)	

<b>tg</b>	(Optional) Configures a TG characteristic profile for route calculation by adjusting the connect cost, byte cost and security TG characteristics. Valid values are <b>high</b> , <b>low</b> , <b>medium</b> , and <b>secure</b> : <ul style="list-style-type: none"> <li>• <b>high</b>—Prefers this link over links with TG profile of <b>medium</b> or <b>low</b>.</li> <li>• <b>low</b>—Prefers this link when links with a TG profile of <b>high</b> or <b>medium</b> is not available.</li> <li>• <b>medium</b>—Prefers this link when links with a TG profile of <b>high</b> is not available.</li> <li>• <b>secure</b>—Prefers this link with when a secure TG is required by the appn class-of-service in use.</li> </ul>
<b>nostart</b>	(Optional) Indicates that the link will not start automatically when defined.

## snasw location

To configure the location of a resource, use the **snasw location** global configuration command. To disable the location of a resource, use the **no** form of this command.

**snasw location** *resource-name* **owning-cp** *cpname*

**no snasw location** *resource-name*

<b>Syntax Description</b>	<i>resource-name</i>	Indicates the fully qualified name of the resource for which location information is being configured (3 to 17 characters).
	<b>owning-cp</b> <i>cpname</i>	Indicates the fully qualified cpname where the resource resides.

## snasw mode

To define a new mode and associate it with an existing class of service (COS), use the **snasw mode** global configuration command. To delete the mode, use the **no** form of this command.

**snasw mode** *mode* **cos** *cos*

**no snasw mode** *mode* **cos** *cos*

<b>Syntax Description</b>	<i>mode</i>	Name of the new mode.
	<b>cos</b> <i>cos</i>	Name of an existing COS, such as #INTER.

## snasw msgdump

To enable automatic dumping of the DLC trace, IPS trace, and problem determination log when a specified SNA Switching Services (SNASw) message is displayed, use the **snasw msgdump** global configuration command. To disable automatic dumping, use the **no** form of this command.

**snasw msgdump** *message*

**no snasw msgdump** *message*

<b>Syntax Description</b>	<i>message</i>	SNASw message to trigger the automatic dump.
---------------------------	----------------	--

## snasw pathswitch

To force an HPR pathswitch for an RTP connection, use the **snasw pathswitch** privileged EXEC command.

**snasw pathswitch** [*rtp-connection-name* | **all**]

<b>Syntax Description</b>	<i>rtp-connection-name</i>	(Optional) Specifies the RTP connection to path-switch. This is an eight-byte string. You can obtain the value for the <i>rtp-connection-name</i> argument from the <b>show snasw rtp</b> command.
	<b>all</b>	(Optional) Specifies that a pathswitch operation will be initiated for every RTP connection managed by the local node.

## snasw pdlog

To control message logging to the console and the SNA problem determination log cyclic buffer, use the **snasw pdlog** global configuration command. To remove previous pdlog configurations, use the **no** form of this command.

**snasw pdlog** [**problem** | **exception** | **info**] [**buffer-size** *buffer-size-value*] [**file** *filename* **timestamp**]

**no snasw pdlog**

<b>Syntax Description</b>	<b>problem</b>	(Optional) Indicates that only problem records are sent to the console. This is the default.
	<b>exception</b>	(Optional) Indicates that both problems and exceptions are sent to the console.
	<b>info</b>	(Optional) Indicates that informational messages and problems and exceptions are sent to the console.
	<b>buffer-size</b> <i>buffer-size-value</i>	(Optional) Indicates the size of the pdlog buffer requested (in kilobytes). The default is 500 KB. The minimum is 10 KB, and the maximum is 16000 KB.

<b>file</b> <i>filename</i>	(Optional) Indicates the URL for writing the pdlog file to a server. Use the following format: <i>protocol://host/path/filename</i> .
<b>timestamp</b>	(Optional) Appends the current date and time to the end of the file when it is dumped.

## snasw port

To specify the DLCs used by SNASw, use the **snasw port** global configuration command. To delete a previously configured port, use the **no** form of this command.

```
snasw port portname [hpr-ip | vdlc ring-group mac mac-address] interfacename [conntype
nohpr | len | dyncplen] [nns-required] [hpr-sap hpr-sap-value] [max-links link-limit-value]
[maxbtu max-btu-size] [sap sap-value] [vname virtual-node-name] [nns] [nostart]
```

```
no snasw port portname
```

Syntax Description	
<i>portname</i>	Indicates the one- to eight-character name for the port. This argument is used to refer to this port in informational messages and the <b>show snasw port</b> command.
<b>hpr-ip</b>	(Optional) Indicates that the port is HPR/IP.
<b>vdlc</b> <i>ring-group</i>	(Optional) Indicates that the port is VDLC. No <i>interfacename</i> is required. The <i>ring-group</i> argument indicates the source-bridge ring group of which this VDLC port is a member.
<b>mac</b> <i>mac-address</i>	(Optional) Indicates that the virtual source MAC address used for the VDLC port.
<i>interfacename</i>	Indicates the name of the interface over which the port will communicate. Allowable interfaces include Token Ring, Ethernet, VLAN, or loopback.
<b>conntype</b> <b>nohpr</b>   <b>len</b>   <b>dyncplen</b>	(Optional) The keyword <b>conntype</b> indicates the connection type for the port. Conntype can be set to one of three values: nohpr, len, or dyncplen. If not configured, HPR-capable links are established. The keyword <b>nohpr</b> indicates that the HPR is not supported but APPN connections with CP-CP sessions are permitted. The keyword <b>len</b> indicates that APPN connections are not allowed; only LEN node-level connectivity is negotiated. The keyword <b>dyncplen</b> (similar to LEN node in functionality) also replaces the cpname. This option is specifically intended for users with XID3-capable devices that send CP names, but whose CP names configured on these devices have not been configured uniquely across the devices. Therefore, a default cpname must be generated to have a properly functioning APPN connection management and directory function.

<b>nns-required</b>	(Optional) Enables configurations with redundant downstream MAC addresses to only allow SNASw nodes that have appropriate upstream connectivity to accept and retain connections from downstream devices. <ul style="list-style-type: none"> <li>When a port is configured with <b>nns-required</b>, the port does not respond to downstream connection requests unless this SNASw node has active CP-CP sessions to an upstream NNS.</li> <li>If a connection has already been made through this SNASw node and then upstream NNS CP-CP connectivity is lost, this SNASw node deactivates all non-HPR links using this port that do not have active LU-LU or ISR sessions.</li> </ul>
<b>hpr-sap</b> <i>hpr-sap-value</i>	(Optional) Indicates the local HPR-SAP value.
<b>max-links</b> <i>link-limit-value</i>	(Optional) Indicates the number of links permitted on this port. When this link limit is reached, the port will not respond to inbound connection requests from stations attempting to connect to this port. Outbound connections are still permitted. Maxlinks can only be coded on VDLC and Virtual Token Ring port types.
<b>maxbtu</b> <i>max-btu-size</i>	(Optional) Indicates the maximum BTU size for the remote end (both inbound and outbound). This value is used in XID3 negotiation. The valid range is 1 to 17800.
<b>sap</b> <i>sap-value</i>	(Optional) Indicates the local SAP value.
<b>vname</b> <i>virtual-node-name</i>	(Optional) Indicates the network qualified virtual node name (3 to 17 characters) of the connection network being defined.
<b>nns</b>	(Optional) Configures the adjacent link as a preferred network node server.  If the primary NN server (uplink) fails, CP-CP sessions are established with a backup, if one is available. When the link to the primary recovers, SNASw retains the CP-CP sessions established with the backup and does not automatically switch back to the primary. To force SNASw to switch back to the primary, use the <b>snasw stop cp-cp</b> command. (If the link to the backup fails, SNASw does switch back to the primary automatically.)
<b>nostart</b>	(Optional) Indicates that the port will not open automatically when defined.

## snasw start

To start SNASw, use the **snasw start** privileged EXEC command.

```
snasw start
```

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

## snasw start cp-cp

To initiate a request to start CP-CP sessions with a partner CP, use the **snasw start cp-cp** privileged EXEC command.

```
snasw start cp-cp cpname
```

<b>Syntax Description</b>	<i>cpname</i>	Indicates the fully qualified CP name of the adjacent node with which CP-CP sessions should be started.
---------------------------	---------------	---

## snasw start link

To start an inactive defined link, use the **snasw start link** privileged EXEC command.

```
snasw start link linkname
```

<b>Syntax Description</b>	<i>linkname</i>	Indicates the name of the link as configured or shown in <b>show snasw link</b> .
---------------------------	-----------------	---

## snasw start port

To start an inactive port, use the **snasw start port** privileged EXEC command.

```
snasw start port portname
```

<b>Syntax Description</b>	<i>portname</i>	Indicates the name of the port as configured or shown in the <b>show snasw port</b> command.
---------------------------	-----------------	--

## snasw stop

To shut down SNASw, use the **snasw stop** privileged EXEC command.

```
snasw stop
```

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

## snasw stop cp-cp

To terminate CP-CP sessions with a partner CP, use the **snasw stop cp-cp** privileged EXEC command.

```
snasw stop cp-cp cpname
```

---

### Syntax Description

*cpname*

Indicates the fully qualified CP name of the adjacent node with which CP-CP sessions should be stopped.

---

## snasw stop link

To stop an active link, use the **snasw stop link** privileged EXEC command.

```
snasw stop link linkname
```

---

### Syntax Description

*linkname*

Indicates the name of the link as configured or shown in the **show snasw link** command.

---

## snasw stop port

To stop an active port, use the **snasw stop port** privileged EXEC command.

```
snasw stop port portname
```

---

### Syntax Description

*portname*

Indicates the name of the port as configured or shown in the **show snasw port** command.

---

## snasw stop session

To terminate an active session, use the **snasw stop session** privileged EXEC command.

```
snasw stop session pcid fqcname netid-destination
```

---

### Syntax Description

*pcid*

Procedure correlator ID in 16-digit hexadecimal form.

*fqcname*

Fully qualified cpname of the node that generates the PCID.

*netid-destination*

Fully qualified primary LU name.

---



## Cisco Transaction Connection Commands

---

This chapter describes the function and syntax of the Cisco Transaction Connection (CTRC) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*.

### clear dbconn connection

To break a client connection to DB2, use the **clear dbconn connection** privileged EXEC command, specifying the ID of the connection you want to terminate.

```
clear dbconn connection connection-id
```

---

**Syntax Description**

---

<i>connection-id</i>	Identification number for client connection to DB2.
----------------------	---

---

### clear dbconn statistic

To clear a specific statistic or all CTRC statistics concerning communications with DB2, use the **clear dbconn statistic** privileged EXEC command.

```
clear dbconn statistic {chains | clientturnaround | connectionsdown | connectionsup | every |  
hostreceived | hostresponse | hostsent | maxconnections }
```

---

**Syntax Description**

---

<b>chains</b>	Clears the number of command chains created between CTRC and DB2.
<b>clientturnaround</b>	Clears statistics for average time from receiving a DB2 client communication to sending that client a response.
<b>connectionsdown</b>	Clears statistics for number of connections down between CTRC and DB2.
<b>connectionsup</b>	Clears statistics for number of connections created between CTRC and DB2.
<b>every</b>	Clears the complete statistics dump between CTRC and DB2.
<b>hostreceived</b>	Clears statistics for number of bytes received from DB2 hosts.

---

<b>hostresponse</b>	Clears statistics for average DB2 host response time.
<b>hostsent</b>	Clears statistics for number of bytes sent to DB2 hosts.
<b>maxconnections</b>	Clears statistics for maximum number of concurrent connections to CICS clients.

## clear txconn connection

To clear a CTRC connection to a CICS client and all associated transactions, use the **clear txconn connection** privileged EXEC command.

```
clear txconn connection connection-id
```

<b>Syntax Description</b>	<i>connection-id</i>	CICS connection identification number.
---------------------------	----------------------	--

## clear txconn statistic

To clear a specific statistic or all CTRC statistics concerning communications with CICS, use the **clear txconn statistic** privileged EXEC command.

```
clear txconn statistic { allocatetime | clientreceived | clientsent | clientturnaround | every |
hostreceived | hostresponse | hostsent | maxconnections | maxtransactions |
totalconnections | totaltransactions }
```

<b>Syntax Description</b>	<b>allocatetime</b>	Clears statistics for average time spent waiting for APPC allocate operation to complete.
	<b>clientreceived</b>	Clears statistics for number of bytes received from CICS clients.
	<b>clientsent</b>	Clears statistics for number of bytes sent to CICS clients.
	<b>clientturnaround</b>	Clears statistics for average time from receiving a CICS client communication to sending that client a response.
	<b>every</b>	Clears every statistic concerning the current router's CTRC communications with CICS.
	<b>hostreceived</b>	Clears statistics for number of bytes received from CICS hosts.
	<b>hostresponse</b>	Clears statistics for average CICS host response time.
	<b>hostsent</b>	Clears statistics for number of bytes sent to CICS hosts.
	<b>maxconnections</b>	Clears statistics for maximum number of concurrent connections to CICS clients.
	<b>maxtransactions</b>	Clears statistics for maximum number of concurrent transactions with CICS hosts.
	<b>totalconnections</b>	Clears statistics for total number of connections to CICS clients.
	<b>totaltransactions</b>	Clears statistics for total number of CICS transactions processed.

## clear txconn transaction

To terminate a specified CICS transaction, use the **clear txconn transaction** privileged EXEC command. This command terminates the conversation with the host and returns DEALLOC\_ABEND\_PROG to the client.

```
clear txconn transaction transaction-id
```

Syntax Description	
<i>transaction-id</i>	ID of the CICS transaction to be cleared.

## dbconn license

To configure client licenses for CTRC connections to DB2 or CICS, use the **dbconn license** global configuration command. To remove the licenses, use the **no** form of this command in privileged EXEC mode.

```
dbconn license license-key connections licensed-connections expiration-date yyyymmdd
```

```
no dbconn license
```

Syntax Description	
<i>license-key</i>	License key obtained from your Cisco representative. The license key is a 32-character hexadecimal string that specifies the maximum number of CICS conversations or DB2 connections allowed for the CTRC router. The license key is generated for a specific router, and is based on the SNA Switching Services cpname for the router. Use the <b>show config   include cpname</b> command to view the cpname so you can provide it when you request the license key.
<b>connections</b> <i>licensed-connections</i>	Number of licensed connections. If the license is for an unlimited number of connections, omit the <b>connections</b> parameter.
<b>expiration-date</b> <i>yyyymmdd</i>	Date when a temporary license key expires, where <i>yyyy</i> is the year expressed in four digits, <i>mm</i> is the month expressed in two digits, and <i>dd</i> is the date expressed in two digits. If the license is for an unlimited time period (permanent license), omit the <b>expiration-date</b> parameter.

## dbconn pem

To configure password expiration management (PEM) support for connections to DB2, use the **dbconn pem** global configuration command. To remove PEM support, use the **no** form of this command.

```
dbconn pem server server-name rlu rlu-name mode mode-name [tpname tp-name]
```

```
no dbconn pem server server-name
```

Syntax Description		
<b>server</b> <i>server-name</i>		Name of the CTRC server that you want to configure for password management.
<b>rlu</b> <i>rlu-name</i>		Host remote LU name the server connects to when performing password management. This RLU ordinarily differs from the RLU values used in <b>dbconn server</b> or <b>txconn destination</b> commands. It may or may not be fully qualified.
<b>mode</b> <i>mode-name</i>		APPC stack mode the server uses when performing password management.
<b>tpname</b> <i>tp-name</i>		(Optional) Name of the PEM transaction program on the host (the APPC Signon transaction program, an architected APPC TP). The default value is \x06301 (0x06F3F0F1 in EBCDIC).

## dbconn ping

To determine whether CTRC servers are successfully connecting to DB2 host databases, use the **dbconn ping** EXEC command.

```
dbconn ping server-name [userid user-id] [password password] [rdbname rdbname]
```

Syntax Description		
<i>server-name</i>		Name of the CTRC server for DB2 communications.
<b>userid</b> <i>user-id</i>		(Optional) User ID used to connect to the DB2 system.
<b>password</b> <i>password</i>		(Optional) Password used to connect to the DB2 system.
<b>rdbname</b> <i>rdbname</i>		(Optional) Name of the relational database to be contacted.

## dbconn server

To configure a CTRC server process for APPC communications with DB2, use the **dbconn server** global configuration command. To disable the server and remove its configuration, use the **no** form of this command.

```
dbconn server server-name [idle-timeout minutes] [ipaddress ip-address] [keepalive attempts
number] [keepalive interval seconds] [mode mode] [port port-number] [rdbname rdbname]
[rlu remote-lu] [tpname tp-name] [window-size bytes] [wlm {off | on}]
```

```
no dbconn server server-name
```

Syntax Description		
<i>server-name</i>		Name of the CTRC server. Server names are user-defined strings up to 16 characters.

<b>idle-timeout</b> <i>idle-timeout</i>	(Optional) Time, in minutes, to wait for an idle client. If there is no activity from the client for this amount of time, the connection is forcibly broken. The time spent in waiting for a response from the DB2 system is not counted, only idle time in between client requests is counted. The maximum is 1440 minutes (24 hours). If no idle timeout is specified, the default is 0 (zero) for no timeout.
<b>ipaddress</b> <i>ip-address</i>	(Optional) IP address used by the CTRC server to receive a connection requesting DB2 communications. When a connection arrives, this IP address is used for matching and selecting the server from multiple configured servers. If you do not specify an IP address, the current server can handle DB2 connectivity requests sent to any IP address on the local router.
<b>keepalive attempts</b> <i>number</i>	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.
<b>keepalive interval</b> <i>seconds</i>	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
<b>mode</b> <i>mode</i>	(Optional) APPC mode used to allocate the conversation to the DB2 system. If no mode is specified, the default is #INTER. Performance might improve if you choose a mode such as IBMRDB. If you specify a mode that does not already exist, CTRC will create it.
<b>port</b> <i>port-number</i>	(Optional) Port used to listen for connections requesting DB2 communications. If no port is specified, the default is 446.
<b>rdbname</b> <i>rdbname</i>	(Optional) DB2 remote database name on the host. When a connection arrives, this name is used to identify and select the appropriate server from multiple configured servers. The string is used to match the RDB name sent by the client in the DRDA data stream at connect time. The default RDB name is an asterisk (*), which indicates that this CTRC server serves any remote database.
<b>rlu</b> <i>remote-lu</i>	(Optional) APPC remote LU used to allocate the connection to the DB2 system. An example is NETA.S103B345. If no remote LU is specified, the default is the configured server name which is set to uppercase and truncated to eight characters. An RLU need not be qualified with a NET ID. If you omit the NET ID, the NET ID of the router's SNA Switching Services control point is used to fully qualify the LU name.
<b>tpname</b> <i>tp-name</i>	(Optional) APPC remote transaction program name used to allocate the conversation to the DB2 system. If no TP name is specified the default is the architected DRDA TP name \x076DB.
<b>window-size</b> <i>bytes</i>	(Optional) TCP/IP receive window size. The maximum window size you can specify is 65,535 bytes, and the default is 4096 bytes.
<b>wlm</b> { <b>off</b>   <b>on</b> }	(Optional) Enables or disables Workload Manager load balancing. The default is "inactive-enabled."

## dbconn tcpserver

To configure a CTRC server process to communicate with IP-enabled DB2 databases, use the **dbconn tcpserver** global configuration command. To disable a server and remove its configuration, use the **no** form of this command.

```
dbconn tcpserver server-name [idle-timeout minutes] [ip ip-address] [keepalive attempts
number] [keepalive interval seconds] [port port-num] [rdbname rdbname]
remote-hostname remote-hostname | remote-ip remote-ip-address [remote-keepalive
attempts number] [remote-keepalive interval seconds] [remote-port remote-port]
[window-size bytes] [wlm { off | on }]
```

```
no dbconn tcpserver server-name
```

Syntax	Description
<i>server-name</i>	Name of the CTRC server being configured for TCP passthrough communications with DB2.
<b>idle-timeout</b> <i>minutes</i>	(Optional) Time in minutes to wait for an idle client. If there is no activity from the client for this amount of time, the connection is forcibly broken. The time spent in waiting for a response from the DB2 system is not counted, only idle time in between client requests is counted. The maximum time is 1440 minutes (24 hours). If no idle timeout is specified, the default is 0 (zero) for no timeout.
<b>ip</b> <i>ip-address</i>	(Optional) IP address for the CTRC tcpserver process being configured. If not specified, the tcpserver receives client requests on all IP addresses configured for the router.
<b>keepalive attempts</b> <i>number</i>	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.
<b>keepalive interval</b> <i>seconds</i>	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
<b>port</b> <i>port-num</i>	(Optional) Port the tcpserver listens on for client requests. The default value is 446. A dbconn server and a dbconn tcpserver can share the same port.
<b>rdbname</b> <i>rdbname</i>	(Optional) DB2 remote database name on the host. When a connection arrives, this name is used to identify and select the appropriate tcpserver from multiple configured tcpserver. The string is used to match the RDB name sent by the client in the DRDA data stream at connect time. The default RDB name is an asterisk (*) which indicates that this CTRC tcpserver serves any remote database.
<b>remote-hostname</b> <i>remote-hostname</i>   <b>remote-ip</b> <i>remote-ip-address</i>	DNS host name of the remote database server to which you want to connect, or the IP address for the host where DB2 resides. You must specify either the name or the IP address of the host.
<b>remote-keepalive attempts</b> <i>number</i>	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the host to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.

<b>remote-keepalive interval</b> <i>seconds</i>	(Optional) The frequency for the CTRC server to send an acknowledgment message to the host to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
<b>remote-port</b> <i>remote-port</i>	(Optional) Host port that listens for tcpserver communications from the router. The default value is 446.
<b>window-size</b> <i>bytes</i>	(Optional) This value is used for the TCP/IP receive window size. If no window size is specified, the default is 4096 bytes.
<b>wlm</b> {off   on}	(Optional) Enables or disables Workload Manager load balancing. The default is “inactive-enabled.”

## show dbconn connection

To display the status of CTRC connections to DB2, use the **show dbconn connection** EXEC command.

```
show dbconn connection [connection-id | server server-name | userid user-id | rdbname
rdb-name]
```

### Syntax Description

<i>connection-id</i>	(Optional) Displays the status of a specified connection.
<b>server</b> <i>server-name</i>	(Optional) Displays connection information for the specified server.
<b>userid</b> <i>user-id</i>	(Optional) Displays connections for the specified user ID.
<b>rdbname</b> <i>rdb-name</i>	(Optional) Displays connections for the specified RDB name.

## show dbconn license

To display the status of CTRC licenses for DB2 communications, use the **show dbconn license** EXEC command.

```
show dbconn license
```

### Syntax Description

This command has no arguments or keywords

## show dbconn ports

To display information about ports that CTRC is using for communications to DB2, use the **show dbconn ports** EXEC command.

```
show dbconn ports
```

### Syntax Description

This command has no arguments or keywords.

## show dbconn server

To display information about CTRC servers configured for DB2 communications, use the **show dbconn server** EXEC command.

```
show dbconn server [server-name]
```

---

### Syntax Description

<i>server-name</i>	(Optional) Specific server for which information should be displayed. When omitted, this command displays information for all CTRC servers configured for DB2 communications on the current router.
--------------------	---

---

## show dbconn statistic

To display all CTRC statistics concerning communications with DB2, use the **show dbconn statistic** privileged EXEC command.

```
show dbconn statistic [kind {histogram | summary}] name {chains | clientturnaround |
connectionsdown | connectionsup | dump | hostreceived | hostresponse | hostsent | latency
| maxconnections}
```

---

### Syntax Description

<b>kind</b> { <b>histogram</b>   <b>summary</b> }	(Optional) Desired format for the statistics to be displayed. Valid values are: <ul style="list-style-type: none"> <li>• <b>histogram</b> displays the named statistic in a graphical format. You cannot use the histogram format when displaying all the statistics (in conjunction with the <b>name dump</b> parameter).</li> <li>• <b>summary</b> displays the named statistic in a tabular format.</li> </ul> If you do not specify the <b>kind</b> parameter, the statistics are displayed in <b>summary</b> format (tabular).
---	---

---

<b>name</b> { <b>chains</b>   <b>clientturnaround</b>   <b>connectionsdown</b>   <b>connectionsup</b>   <b>dump</b>   <b>hostreceived</b>   <b>hostresponse</b>   <b>hostsent</b>   <b>latency</b>   <b>maxconnections</b> }	<p>The statistics you can display with the <b>name</b> keyword are:</p> <ul style="list-style-type: none"> <li>• <b>chains</b> displays statistics for number of chains created.</li> <li>• <b>clientturnaround</b> displays statistics for average time from receiving a DB2 client communication to sending that client a response.</li> <li>• <b>connectionsdown</b> displays the number of connections completed between CTRC and DB2 during the indicated time period.</li> <li>• <b>connectionsup</b> displays the number of connections created between CTRC and DB2 during the indicated time period.</li> <li>• <b>dump</b> displays a compact statistics summary, in tabular format, for the last 24 hours. The statistics dump includes all the individual statistics you can specify with the <b>name</b> keyword.</li> <li>• <b>hostreceived</b> displays the total number of bytes the router has received from DB2 hosts during the indicated time period.</li> <li>• <b>hostresponse</b> displays the average host response time in seconds for DB2 connections during the indicated time period.</li> <li>• <b>hostsent</b> displays the total number of bytes the router has sent to DB2 hosts during the indicated time period.</li> <li>• <b>latency</b> displays the average amount of time in seconds used by the txconn server per CICS client request (clientturnaround minus hostresponse).</li> <li>• <b>maxconnections</b> displays the maximum number of concurrent connections to CICS clients established during the indicated time period.</li> <li>• <b>maxtransactions</b> displays the maximum number of concurrent CICS transactions during the indicated time period.</li> <li>• <b>totalconnections</b> displays the total number of connections to CICS clients used during the indicated time period.</li> <li>• <b>totaltransactions</b> displays the total number of CICS transactions processed during the indicated time period.</li> </ul>
---	--

## show dbconn wlm

To display information about a CTRC server that is configured to use Workload Manager for DB2 communications, use the **show dbconn wlm EXEC** command.

```
show dbconn wlm server-name
```

### Syntax Description

<i>server-name</i>	Name of the CTRC server that is configured to use Workload Manager to manage DB2 communications.
--------------------	--

## show txconn connection

To display a list of all of the router's CTRC connections to CICS clients, a list of a specified CTRC server's connections to CICS clients, or detailed status information for a specific CTRC connection to a CICS client, use the **show txconn connection** EXEC command.

```
show txconn connection [connection-id | server server-name]
```

<b>Syntax Description</b>	<i>connection-id</i>	(Optional) Specifies a CTRC connection to a CICS client for which to display detailed status information.
	<b>server</b> <i>server-name</i>	(Optional) Specifies a CTRC server for which to list connections to CICS clients.

## show txconn destination

To display a list of all of the current router's CICS destinations for CTRC, or to display detailed status information for a specified CTRC CICS destination, use the **show txconn destination** EXEC command.

```
show txconn destination [destination-name]
```

<b>Syntax Description</b>	<i>destination-name</i>	(Optional) CTRC destination for which to display detailed status information. A destination is defined by a unique remote LU and mode pair.
---------------------------	-------------------------	---

## show txconn license

To show the status of licenses used for CTRC, use the **show txconn license** EXEC command.

```
show txconn license
```

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

## show txconn route

To display a list of all CTRC routes defined for specified CICS transaction IDs, or to display a particular CTRC server's routes to CICS, use the **show txconn route** EXEC command.

```
show txconn route [server server-name]
```

<b>Syntax Description</b>	<b>server</b> <i>server-name</i>	(Optional) Server for which you wish to display routing information. If not specified, a list of all CICS communications routes for CTRC servers on the current router is displayed.
---------------------------	----------------------------------	--

## show txconn server

To display information about the current router's CTRC servers for CICS communications, or to display detailed status information for a single CTRC server, use the **show txconn server** EXEC command.

```
show txconn server [server-name]
```

<b>Syntax Description</b>	<i>server-name</i>	(Optional) CTRC server for which to display detailed status information. When omitted, a list of CTRC servers is displayed.
---------------------------	--------------------	---

## show txconn statistic

To display information about the current router's CTRC communications with CICS, use the **show txconn statistic** EXEC command.

```
show txconn statistic [kind {histogram | summary}] name {activeconnections |  
activetransactions | allocatetime | clientreceived | clientsent | clientturnaround | dump |  
hostreceived | hostresponse | hostsent | latency | maxconnections | maxtransactions |  
totalconnections | totaltransactions}
```

<b>Syntax Description</b>	<b>kind</b> { <b>histogram</b>   <b>summary</b> }	(Optional) Desired format for the statistics to be displayed. Valid values are: <ul style="list-style-type: none"> <li><b>histogram</b> displays the named statistic in a graphical format. You cannot use the histogram format when displaying all the statistics (in other words, in conjunction with the <b>name dump</b> parameter).</li> <li><b>summary</b> displays the named statistic in a tabular format.</li> </ul> If you do not specify the <b>kind</b> parameter, the statistics are displayed in <b>summary</b> format (tabular).
---------------------------	---	---

<b>name</b> { <b>activeconnections</b>   <b>activetransactions</b>   <b>allocatetime</b>   <b>clientreceived</b>   <b>clientsent</b>   <b>clientturnaround</b>   <b>dump</b>   <b>hostreceived</b>   <b>hostresponse</b>   <b>hostsent</b>   <b>latency</b>   <b>maxconnections</b>   <b>maxtransactions</b>   <b>totalconnections</b>   <b>totaltransactions</b> }	Specific statistic to display. Valid values are: <ul style="list-style-type: none"> <li>• <b>activeconnections</b> displays the number of connections to CICS clients currently active.</li> <li>• <b>activetransactions</b> displays the number of CICS transactions currently being processed.</li> <li>• <b>allocatetime</b> displays the average time in seconds spent waiting for APPC allocate operation to complete.</li> <li>• <b>clientreceived</b> displays the total number of bytes received from CICS clients during the indicated time period.</li> <li>• <b>clientsent</b> displays the total number of bytes sent to CICS clients during the indicated time period.</li> <li>• <b>clientturnaround</b> displays the average time in seconds from receiving a request from a CICS client to sending that client a response during the indicated time period.</li> <li>• <b>dump</b> displays a compact statistics summary, in tabular format, for the last 24 hours. The statistics include all the individual statistics you can specify with the <b>name</b> parameter except the <b>activeconnections</b> and <b>activetransactions</b> data.</li> <li>• <b>hostreceived</b> displays the total number of bytes received from hosts for CICS connections during the indicated time period.</li> <li>• <b>hostresponse</b> displays the average host response time in seconds for CICS connections during the indicated time period.</li> <li>• <b>hostsent</b> displays the total number of bytes sent to hosts for CICS connections during the indicated time period.</li> <li>• <b>latency</b> displays the average amount of time in seconds used by the txconn server per CICS client request (<b>clientturnaround</b> minus <b>hostresponse</b>).</li> <li>• <b>maxconnections</b> displays the maximum number of concurrent connections to CICS clients during the indicated time period.</li> <li>• <b>maxtransactions</b> displays the maximum number of concurrent CICS transactions during the indicated time period.</li> <li>• <b>totalconnections</b> displays the total number of connections to CICS clients used during the indicated time period.</li> <li>• <b>totaltransactions</b> displays the total number of CICS transactions processed during the indicated time period.</li> </ul>
--	--

## show txconn transaction

To display a list of all the current router's CTRC transactions with CICS, a specified CTRC server's transactions, or a specified CICS client connection's transactions, use the **show txconn transaction** EXEC command.

```
show txconn transaction [server server-name | connection connection-id | transaction-id]
```

Syntax Description		
<b>server</b> <i>server-name</i>	(Optional) Specifies a CTRC server for which to display a list of transactions.	
<b>connection</b> <i>connection-id</i>	(Optional) Specifies a CICS client connection to CTRC for which to display a list of transactions.	
<i>transaction-id</i>	(Optional) Specifies an individual transaction for which to display detailed status information.	

## txconn destination

To configure a CTRC destination, use the **txconn destination** global configuration command. To remove the configuration for a txconn destination, use the **no** form of this command.

```
txconn destination destination-name rlu rlu-name mode mode-name
```

```
no txconn destination destination-name
```

Syntax Description		
<i>destination-name</i>	Name of the destination being defined or added to. This name is used in the route configuration command to identify the destination for the route.  If the destination does not exist, it is created; if it exists, the <b>rlu</b> and <b>mode</b> parameters are added as an additional routing target for this destination. When a destination contains multiple routing targets, it is like configuring a cluster where the various targets are chosen on a round-robin basis for load balancing.	
<b>rlu</b> <i>rlu-name</i>	Remote LU name on the host. This parameter defines to which remote LU the server will connect when using this destination. A remote LU corresponds directly to a CICS region. The value you enter here should match your VTAM APPLID.	
<b>mode</b> <i>mode-name</i>	Name of the APPC mode. This parameter defines which mode the server will use for its APPC connections when using this destination. If the mode you specify does not already exist, CTRC will create it.	

## txconn license

To license a Cisco router for CTRC communications with CICS or DB2, use the **txconn license** global configuration command. To remove the license, use the **no** form of this command.

```
txconn license license-key connections licensed-connections expiration-date yyyymmdd
```

```
no txconn license
```

<b>Syntax Description</b>	<i>license-key</i>	License key obtained from your Cisco representative. The license key is a 32-character hexadecimal string that specifies the maximum number of CICS conversations or DB2 connections allowed for the CTRC router. The license key is generated for a specific router, and is based on the SNA Switching Services cpname for the router. Use the <b>show config   include cpname</b> command to view the cpname so you can provide it when you request the license key.
	<b>connections</b> <i>licensed-connections</i>	Number of licensed connections. If the license is for an unlimited number of connections, omit the <b>connections</b> parameter.
	<b>expiration-date</b> <i>yyyymmdd</i>	Date when a temporary license key expires, where <i>yyyy</i> is the year expressed in four digits, <i>mm</i> is the month expressed in two digits, and <i>dd</i> is the date expressed in two digits. If the license is for an unlimited time period (permanent license), omit the <b>expiration-date</b> parameter.

## txconn ping

To test communications between the CTRC router and a CTRC destination (a host defined by a pair of RLU and mode values), use the **txconn ping EXEC** command.

**txconn ping** *destination-name*

<b>Syntax Description</b>	<i>destination-name</i>	Specifies the CICS system for which to test communications.
---------------------------	-------------------------	---

## txconn route

To configure a CTRC route that will transmit specified transactions to a particular CICS destination, use the **txconn route** global configuration command. To remove the configuration of a CTRC route, use the **no** form of this command.

**txconn route** [**server** *server-name*] **tranid** *transaction-id* **destination** *destination-name*

**no txconn route** [**server** *server-name*] **tranid** *transaction-id*

<b>Syntax Description</b>	<b>server</b> <i>server-name</i>	(Optional) Name of the CTRC server to which this route applies. If omitted, this route is applied to all CTRC servers on the current router that are configured for communication with CICS.
	<b>tranid</b> <i>transaction-id</i>	CICS transaction ID (a TP name). When the server processes a transaction that uses this transaction ID, the server routes the transaction using this route entry.
	<b>destination</b> <i>destination-name</i>	Name of the destination to which the transaction is routed.

## txconn server

To configure a CTRC server for communications with CICS, use the **txconn server** global configuration command. To disable a CTRC server, use the **no** form of this command.

```
txconn server server-name destination destination-name [access { cics | comti }] [ccsid number]
[client-timeout minutes] [fold { on | off }] [host-timeout minutes] [ipaddress ip-address]
[keepalive attempts number] [keepalive interval seconds] [port port-number] [target
{ cics | ims-tm }] [window-size bytes]
```

```
no txconn server server-name
```

Syntax Description	
<i>server-name</i>	Name of the server being defined. This name is used in other commands to identify the server being administered.
<b>destination</b> <i>destination-name</i>	Name of the server's default destination. Any transactions whose <i>tranid</i> is not associated with a particular route will be routed to this destination. The destination must already be defined when configuring the server.
<b>access</b> { <b>cics</b>   <b>comti</b> }	(Optional) Indicates whether <i>server-name</i> supports IBM CICS (Universal Client or TXSeries) or Microsoft COMTI clients. If this value is not specified, a default of CICS is used.
<b>ccsid</b> <i>number</i>	(Optional) The Coded Character Set Identifier. This is used for TXSeries clients.
<b>client-timeout</b> <i>minutes</i>	(Optional) Number of minutes of client connection inactivity after which the server decides the client has gone away. When this happens the server closes the client connection. If no client timeout is specified, the default is 0 (zero) for no timeout.
<b>fold</b> { <b>on</b>   <b>off</b> }	(Optional) Enables/disables the fold program. Default is on. CTRC folds the CICS program name to uppercase.
<b>host-timeout</b> <i>minutes</i>	(Optional) Number of minutes of host connection inactivity after which the server decides the host has gone away. When this happens the server closes the host connection. If no host timeout is specified, the default is 0 (zero) for no timeout.
<b>ipaddress</b> <i>ip-address</i>	(Optional) TCP/IP network address for which the server accepts connections. If this parameter is omitted, the server accepts connections for any IP address, like a wildcard address. If multiple servers are configured to listen on the same port, they must each specify a different IP address. If a server is configured with the IP address omitted, no other servers may listen on the same port. So, on a given port, you may configure either 1 wildcard IP address server, or <i>n</i> address-specific servers, where <i>n</i> is 1 or more.
<b>keepalive attempts</b> <i>number</i>	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.
<b>keepalive interval</b> <i>seconds</i>	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.

---

<b>port</b> <i>port-number</i>	(Optional) TCP/IP port number on which the server listens. If no IP address is specified, only one server can listen on a port. Multiple servers can use the same port number if the combination of IP address and port number is unique to each server. If the port number is omitted, the server listens on port 1435.
<b>target</b> { <b>cics</b>   <b>ims-tm</b> }	(Optional) Indicates whether the host connection is to a CICS or IMS transaction server. The default is cics.
<b>window-size</b> <i>bytes</i>	(Optional) Size, in bytes, of the TCP/IP window for incoming CICS client connections. If no window size is specified, the default is 4096 bytes.

---



# Cisco Mainframe Channel Connection Commands

---

This chapter describes the function and syntax of the Cisco Mainframe Channel Connection (CMCC) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*.

## adapter

To configure internal adapters, use the **adapter** internal LAN interface configuration command. To remove an internal adapter, use the **no** form of this command.

```
adapter adapter-number [mac-address]
```

```
no adapter adapter-number [mac-address]
```

---

### Syntax Description

<i>adapter-number</i>	Number in the range 0 to 31 that uniquely identifies the internal adapter (relative adapter number) for all internal LANs of the same type on the CMCC adapter. When configuring CSNA, this value corresponds to the ADAPNO parameter defined in the Virtual Telecommunications Access Method (VTAM) Extended Communications Adapter (XCA) Major Node.
<i>mac-address</i>	(Optional) Media Access Control (MAC) address for this internal adapter. This is a hexadecimal value in the form <i>xxxx.xxxx.xxxx</i> .

---

## channel-protocol

To define a data rate of either 3 MBps or 4.5 MBps for Parallel Channel Interfaces, use the **channel-protocol** interface configuration command. To return to the default rate of 3 MBps, use the **no** form of this command.

```
channel-protocol [s | s4]
```

```
no channel-protocol
```

<b>Syntax Description</b>	<b>s</b>	(Optional) Specifies a data rate of 3 MBps.
	<b>s4</b>	(Optional) Specifies a data rate of 4.5 MBps.

## clear extended counters

To clear the extended interface counters associated with CMCC features, use the **clear extended counters** EXEC command.

```
clear extended counters [channel slot/port [csna | icmp-stack | ip-stack | llc2 | statistics |
tcp-connections | tcp-stack | tg | tn3270-server | udp-stack]]
```

<b>Syntax Description</b>	<b>channel</b>	(Optional) Specifies a channel interface.
	<i>slot</i>	(Optional) Slot number.
	<i>port</i>	(Optional) Port number.
	<b>csna</b>	(Optional) Clears CSNA feature counters.
	<b>icmp-stack</b>	(Optional) Clears ICMP stack counters.
	<b>ip-stack</b>	(Optional) Clears IP stack counters.
	<b>llc2</b>	(Optional) Clears LLC2 counters.
	<b>statistics</b>	(Optional) Clears subchannel statistic counters.
	<b>tcp-connections</b>	(Optional) Clears TCP connection counters.
	<b>tcp-stack</b>	(Optional) Clears TCP stack counters.
	<b>tg</b>	(Optional) Clears TG counters.
	<b>tn3270-server</b>	(Optional) Clears TN3270 Server counters.
	<b>udp-stack</b>	(Optional) Clears UDP stack counters.

## exception slot

To provide a core dump of a CMCC adapter, use the **exception slot** global configuration command. To disable the core dump, use the **no** form of this command.

```
exception slot [slot] protocol://host/filename
```

```
no exception slot [slot] protocol://host/filename
```

<b>Syntax Description</b>	<i>slot</i>	(Optional) Slot number of the CMCC adapter. If no <i>slot</i> is specified, all installed CMCC adapters will output a core dump when they halt unexpectedly.
	<i>protocol</i>	Protocol for transferring the file. Currently, the only allowed value is FTP.
	<i>host</i>	Name or IP address of the host that receives the core dump information.
	<i>filename</i>	Filename on the host that receives the core dump information. The maximum name length is 31 characters. When written to the host, <i>slot</i> is automatically appended, where <i>slot</i> is the slot number.

## interface channel

To specify a channel-attached interface and enter interface configuration mode, use the **interface channel** global configuration command.

```
interface channel slot/port
```

Syntax Description	slot	Slot number where the CMCC adapter is located.
	port	Interface where the CMCC adapter is located.

## lan

To configure an internal LAN on a CMCC adapter interface and enter the internal LAN configuration mode, use the **lan** interface configuration command. To remove an internal LAN interface, use the **no** form of this command.

```
lan type lan-id
```

```
no lan type lan-id
```

Syntax Description	type	Interface type for this internal LAN: <b>tokenring</b> .
	lan-id	Number 0 to 31 that uniquely identifies the internal LAN on this CMCC adapter. This value must be unique between all internal LANs of the same interface type on a CMCC adapter.

## max-llc2-sessions

To specify the maximum number of LLC2 sessions supported on the CMCC adapter, use the **max-llc2-sessions** interface configuration command. To restore the default value, use the **no** form of this command.

```
max-llc2-sessions number
```

```
no max-llc2-sessions number
```

Syntax Description	number	A value in the range 1 to 6000 LLC sessions. If this command is not configured, the default is 256 sessions.
--------------------	--------	--

name

## name

To assign a name to the internal adapter, use the **name** internal adapter configuration command. To remove the name assigned to an internal adapter, use the **no name** form of this command.

**name** *name*

**no name** *name*

Syntax Description	<i>name</i>
	Name that identifies this internal adapter. The name consists of up to 8 characters (not including blanks).

## show controllers channel

To display CPA-specific information, including the currently loaded microcode, use the **show controllers channel** EXEC command.

**show controllers channel** [*slot/port*]

Syntax Description	<i>slot</i>	(Optional) Slot number.
	<i>port</i>	(Optional) Interface number.

## show extended channel connection-map llc2

To display the number of active LLC2 connections for each SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP, use the **show extended channel connection-map llc2** privileged EXEC command.

**show extended channel** *slot/port* **connection-map llc2**

Syntax Description	<i>slot</i>	Slot number.
	<i>port</i>	Port number.
<b>connection-map llc2</b>	Displays a connection map of LLC2 connections.	

## show extended channel icmp-stack

To display information about the Internet Control Message Protocol (ICMP) stack running on the CMCC channel interfaces, use the **show extended channel icmp-stack** EXEC command.

**show extended channel** *slot/port* **icmp-stack** [*ip-address*]

**Syntax Description**

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<i>ip-address</i>	(Optional) IP address specified by the <b>offload</b> interface configuration command or the <b>tn3270-server pu</b> command.

## show extended channel ip-stack

To display information about the IP stack running on CMCC channel interfaces, use the **show extended channel ip-stack** EXEC command.

```
show extended channel slot/port ip-stack [ip-address]
```

**Syntax Description**

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<i>ip-address</i>	(Optional) IP address specified by the <b>offload</b> interface configuration command or the <b>tn327-server pu</b> command.

## show extended channel lan

To display the internal LANs and adapters configured on a CMCC adapter, use the **show extended channel lan** EXEC command.

```
show extended channel slot/port lan [tokenring [lan-id [adapno]]]
```

**Syntax Description**

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<i>tokenring</i>	(Optional) Specify CMCC internal LAN type to be displayed.
<i>lan-id</i>	(Optional) Specify the CMCC internal LAN number to be displayed.
<i>adapno</i>	(Optional) Specify the CMCC internal adapter number on the selected internal LAN to be displayed.

## show extended channel llc2

To display information about the LLC2 sessions running on the CMCC adapter interfaces, use the **show extended channel llc2** EXEC command.

```
show extended channel slot/port llc2 [admin | oper | stats] [lmac [lsap [rmac [rsap]]]]
```

**Syntax Description**

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<b>admin</b>	(Optional) Shows configured values. This is the default.

<b>oper</b>	(Optional) Shows operational values for: <ul style="list-style-type: none"> <li>• Internal adapters</li> <li>• SAPs opened on the internal adapters</li> <li>• LLC2 connections on the internal adapters</li> </ul>
<b>stats</b>	(Optional) Displays statistics for: <ul style="list-style-type: none"> <li>• Internal adapters</li> <li>• SAPs opened on the internal adapters</li> <li>• LLC connections on the internal adapters</li> </ul>
<i>lmac</i>	(Optional) Local MAC address.
<i>lsap</i>	(Optional) Local service access point (SAP) address, 0 to 256.
<i>rmac</i>	(Optional) Remote MAC address.
<i>rsap</i>	(Optional) Remote SAP address, 0 to 256.

## show extended channel max-llc2-sessions

To display information about the number of LLC2 sessions supported on the CMCC adapter, use the **show extended channel max-llc2-sessions** privileged EXEC command.

```
show extended channel slot/port max-llc2-sessions
```

### Syntax Description

<i>slot</i>	Slot number.
<i>port</i>	Port number.

## show extended channel statistics

To display statistical information about subchannels on the physical interface of a CMCC adapter, use the **show extended channel statistics** EXEC command. This command displays information that is specific to the interface channel devices. The information is generally useful only for diagnostic tasks performed by technical support personnel.

```
show extended channel slot/port statistics [path [device-address]] [connected]
```

### Syntax Description

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<i>path</i>	(Optional) Hexadecimal value in the range 0x0000 to 0xFFFF. This value specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch): one digit for the control unit address, and one digit for the channel logical address.

<i>device-address</i>	(Optional) Hexadecimal value in the range 0x00 to 0xFE. This value is the unit address associated with the control unit number and path as specified in the host IOCP file. For CLAW and offload support, the device address must have an even value.
<b>connected</b>	(Optional) For each backup group, only display information about the active subchannel or the first subchannel defined in the group if none are active.

## show extended channel subchannel

To display information about the CMCC adapter physical interfaces, use the **show extended channel subchannel** EXEC command. This command displays information that is specific to the interface channel connection. The information displayed is generally useful only for diagnostic tasks performed by technical support personnel.

```
show extended channel slot/port subchannel [connected]
```

### Syntax Description

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<b>connected</b>	(Optional) For each backup group, displays information about the active subchannel or the first subchannel defined in the group if none are active.

## show extended channel tcp-connections

To display information about the Transmission Control Protocol (TCP) sockets on a channel interface, use the **show extended channel tcp-connections** EXEC command.

```
show extended channel slot/port tcp-connections [[loc-ip-addr [loc-port [rem-ip-addr  
[rem-port]]] [detail | summary]
```

### Syntax Description

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<b>tcp-connections</b>	Specifies TCP connections display.
<i>loc-ip-addr</i>	(Optional) Local IP address. IP address of the local connection endpoint. Restricts the output to those connections with a matching local IP address.
<i>loc-port</i>	(Optional) Local TCP port. This is the TCP port of the local connection endpoint. Restricts the output to those connections with a matching local TCP port. An asterisk (*) is a wildcard that matches every port.
<i>rem-ip-addr</i>	(Optional) Remote IP address. IP address of the remote connection endpoint. Restricts the output to those connections with a matching remote IP address.
<i>rem-port</i>	(Optional) Remote TCP port. TCP port of the remote connection endpoint. Restricts the output to those connections with a matching remote TCP port.
<b>detail</b>	(Optional) Prints detailed information about every matching connection.
<b>summary</b>	(Optional) This is the default. Prints a summary of all matching connections.

## show extended channel tcp-stack

To display information about the TCP stack running on CMCC adapter interfaces, use the **show extended channel tcp-stack** EXEC command.

```
show extended channel slot/port tcp-stack [ip-address]
```

Syntax Description		
	<i>slot</i>	Slot number.
	<i>port</i>	Port number.
	<b>tcp-stack</b>	Specifies <b>tcp stack</b> display.
	<i>ip-address</i>	(Optional) IP address specified by the <b>offload</b> interface configuration command or the <b>tn327-server pu</b> command.

## show extended channel udp-listeners

To display information about the User Datagram Protocol (UDP) listener sockets running on the CMCC adapter interfaces, use the **show extended channel udp-listeners** EXEC command.

```
show extended channel slot/port udp-listeners [ip-address]
```

Syntax Description		
	<i>slot</i>	Slot number.
	<i>port</i>	Port number.
	<b>udp-listeners</b>	Specifies UDP listener port display.
	<i>ip-address</i>	(Optional) IP address specified by the <b>offload</b> interface configuration command or the <b>tn3270-server pu</b> command.

## show extended channel udp-stack

To display information about the UDP stack running on the CMCC adapter interfaces, use the **show extended channel udp-stack** EXEC command.

```
show extended channel slot/port udp-stack [ip-address]
```

Syntax Description		
	<i>slot</i>	Slot number.
	<i>port</i>	Port number.
	<b>udp-stack</b>	Selects UDP stack display.
	<i>ip-address</i>	(Optional) IP address specified by the <b>offload</b> interface configuration command or the <b>tn3270-server pu</b> command.

## show interfaces channel

To display information about the CMCC adapter interfaces, use the **show interfaces channel** privileged EXEC command. This command displays information that is specific to the interface hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

```
show interfaces channel slot/port [accounting]
```

Syntax Description		
	<i>slot</i>	Slot number.
	<i>port</i>	Port number.
	<b>accounting</b>	(Optional) Displays interface accounting information.

## shutdown (CMCC)

To shut down an interface or the virtual interface on the CMCC adapter when you are in interface configuration mode, use the **shutdown** CMCC command. The **shutdown** TN3270 server command also shuts down TN3270 entities, such as PU, DLUR, and DLUR SAP, depending on which configuration mode you are in when the command is issued. To restart the interface or entity, use the **no** form of this command. The entity affected depends on the mode in which the command is issued.

```
shutdown
```

```
no shutdown
```

Syntax Description	
	This command has no arguments or keywords.

## state-tracks-signal

To allow the channel interface state to track the state of the physical interface signal on a Channel Port Adapter (CPA), use the **state-tracks-signal** interface configuration command. To disable tracking of the physical interface signal on a Channel Port Adapter interface, use the **no** form of this command.

```
state-tracks-signal
```

```
no state-tracks-signal
```

Syntax Description	
	This command has no arguments or keywords.





## CLAW and TCP/IP Offload Commands

This chapter describes the function and syntax of the CLAW and TCP/IP offload commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*.

### claw (primary)

To configure a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configure individual members of a CLAW backup group for the IP Host Backup feature, use the **claw** interface configuration command. To remove the CLAW device, use the **no** form of this command.

```
claw path device-address ip-address host-name device-name host-app device-app [broadcast]  
[backup]
```

```
no claw path device-address
```

Syntax Description	
<i>path</i>	Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
<i>device-address</i>	Hexadecimal value in the range 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even value.
<i>ip-address</i>	IP address specified in the HOME statement of the host TCP/IP application configuration file.
<i>host-name</i>	Host name specified in the device statement in the host TCP/IP application configuration file.
<i>device-name</i>	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.

<i>host-app</i>	Host application name as specified in the host application file. If connected to the IBM TCP host offerings, or if the CLAW packing feature is not enabled on the mainframe TCPIP stack, this value will be <b>tcpip</b> , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application. The value <b>packed</b> can be used for the <i>host-app</i> parameter to enable the CLAW packing feature.
<i>device-app</i>	CLAW workstation application specified in the host TCPIP application. If connected to the IBM TCP host offerings, or if the CLAW packing feature is not enabled on the mainframe TCPIP stack, this value will be <b>tcpip</b> , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application. The value <b>packed</b> can be used for the <i>device-app</i> parameter to enable the CLAW packing feature.
<b>broadcast</b>	(Optional) Enables broadcast processing for this subchannel.
<b>backup</b>	(Optional) Enables this CLAW connection to be used as part of a backup group of CLAW connections for the specified IP address.

## claw (backup)

To configure a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and configure individual members of a CLAW backup group for the IP Host Backup feature, use the **claw** command in IP host backup configuration mode. To remove the CLAW device, use the **no** form of this command.

**claw** *path device-address ip-address host-name device-name host-app device-app* [**broadcast**]

**no claw** *device-address*

### Syntax Description

<i>path</i>	Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
<i>device-address</i>	Hexadecimal value in the range 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even value.
<i>ip-address</i>	IP address specified in the HOME statement of the host TCP/IP application configuration file.
<i>host-name</i>	Host name specified in the device statement in the host TCP/IP application configuration file.
<i>device-name</i>	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.

<i>host-app</i>	Host application name as specified in the host application file. When connected to the IBM TCP host offerings, this value will be <b>tcpip</b> , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application.
<i>device-app</i>	CLAW workstation application specified in the host TCPIP application. When connected to the IBM TCP host offerings, this value will be <b>tcpip</b> , which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application.
<b>broadcast</b>	(Optional) Enables broadcast processing for this subchannel.

## offload (primary)

To configure an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and configure individual members of an Offload backup group for the IP Host Backup feature, use the **offload** interface configuration command. To cancel the offload task on the CMCC adapter, use the **no offload** form of this command.

**offload** *path device-address ip-address host-name device-name host-ip-link device-ip-link host-api-link device-api-link* [**broadcast**] [**backup**]

**no offload** *path device-address*

Syntax Description	
<i>path</i>	Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
<i>device-address</i>	Hexadecimal value in the range 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even value.
<i>ip-address</i>	IP address specified in the host TCP/IP application configuration file.
<i>host-name</i>	Host name specified in the device statement in the host TCP/IP application configuration file.
<i>device-name</i>	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.
<i>host-ip-link</i>	CLAW host link name for the IP link as specified by the host application. For IBM VM and VMS TCP/IP stacks, this value is <b>tcpip</b> . When used with other applications, this value must match the value coded in the host application.
<i>device-ip-link</i>	CLAW workstation link name for the IP link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is <b>tcpip</b> . When used with other applications, this value must match the value coded in the host application.

<i>host-api-link</i>	CLAW host link name for the API link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is <b>tcpip</b> . When used with other applications, this value must match the value coded in the host application.
<i>device-api-link</i>	Offload link name for the API link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is <b>api</b> . When used with other applications, this value must match the value coded in the host application.
<b>broadcast</b>	(Optional) Enables broadcast processing for this subchannel.
<b>backup</b>	(Optional) Enables this offload connection to be used as part of a backup group of offload connections for the specified IP address.

## offload alias

To assign a virtual IP address to a real IP address for an offload device on a CMCC adapter, use the **offload alias** interface configuration command. To remove the alias IP address, use the **no** form of this command.

**offload alias** *real-ip alias-ip*

**no offload alias** *real-ip alias-ip*

### Syntax Description

<i>real-ip</i>	Real IP address of the offload-supported device.
<i>alias-ip</i>	Virtual IP address for the offload-supported device.

## offload (backup)

To configure a backup group of Offload devices, use the **offload** IP host backup configuration command. To cancel the offload task on the CMCC adapter, use the **no** form of this command.

**offload** *device-address ip-address host-name device-name host-ip-link device-ip-link host-api-link device-api-link* [**broadcast**]

**no offload** *path device-address*

### Syntax Description

<i>device-address</i>	Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
<i>ip-address</i>	Hexadecimal value in the range 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even value.
<i>host-name</i>	Host name specified in the device statement in the host TCP/IP application configuration file.

<i>device-name</i>	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.
<i>host-ip-link</i>	Host link name for the IP link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is <b>tcpip</b> . When used with other applications, this value must match the value coded in the host application.
<i>device-ip-link</i>	Workstation link name for the IP link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is <b>tcpip</b> . When used with other applications, this value must match the value coded in the host application.
<i>host-api-link</i>	Host link name for the API link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is <b>tcpip</b> . When used with other applications, this value must match the value coded in the host application.
<i>device-api-link</i>	Offload link name for the API link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is <b>api</b> . When used with other applications, this value must match the value coded in the host application.
<b>broadcast</b>	(Optional) Enables broadcast processing for this subchannel.

## path

To specify one or more data paths for the IP host backup, use the **path** interface configuration command. To delete a single path, use the **no path** form of this command.

**path** *path...*

**no path** *path*

### Syntax Description

<i>path</i>	Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
-------------	---

## show extended channel backup

To display information about the CLAW and offload commands for each backup group configured on CMCC channel interfaces, use the **show extended channel backup** privileged EXEC command.

**show extended channel** *slot/port backup* [*ip-address*]

### Syntax Description

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<b>backup</b>	Displays all <b>claw</b> or <b>offload</b> commands associated with the backup group.
<i>ip-address</i>	(Optional) Displays information about all devices in the backup group defined by the <i>ip-address</i> argument.

## show extended channel packing names

To display CLAW packing names and their connection state, use the **show extended channel packing names EXEC** command.

```
show extended channel slot/port packing names [path [device-address]]
```

Syntax Description		
<i>slot</i>		Slot number.
<i>port</i>		Port number.
<i>path</i>		(Optional) Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
<i>device-address</i>		(Optional) Hexadecimal value in the range 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even value.

## show extended channel packing stats

To display CLAW packing statistics, use the **show extended channel packing stats EXEC** command.

```
show extended channel slot/port packing stats [path [device-address]]
```

Syntax Description		
<i>slot</i>		Slot number.
<i>port</i>		Port number.
<i>path</i>		(Optional) Hexadecimal value in the range 0000 to FFFF. This specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch): one digit for the control unit address, and one digit for the channel logical address. If not specified, the control unit address and channel logical address default to 0.
<i>device-address</i>		(Optional) Hexadecimal value in the range 00 to FE. This value is the unit address associated with the control unit number and path as specified in the host IOCP file. For CLAW and offload support, the device address must have an even value.



## CMPC, CMPC+, and CSNA Commands

This chapter describes the function and syntax of the CMPC, CMPC+, and CSNA commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*.

### cmpc

To configure a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel, use the **cmpc** interface configuration command. To remove a subchannel definition and to deactivate the transmission group, use the **no** form of this command.

```
cmpc path device tg-name {read | write}
```

```
no cmpc path device
```

#### Syntax Description

<i>path</i>	Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
<i>device</i>	Hexadecimal value in the range of 00 to FF. This is the unit address associated with the control unit number and path as specified in the host IOCP file.
<i>tg-name</i>	Name of the CMPC or CMPC+ TG. The maximum length of the name is 8 characters.
<b>read</b>	Same read value as specified in the TRL major node.
<b>write</b>	Same write value as specified in the TRL major node.

### csna

To configure SNA support on a CMCC physical channel interface, use the **csna** interface configuration command. This command is used to specify the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe. To delete the CSNA device path, use the **no** form of this command.

```
csna path device [maxpiu value] [time-delay value] [length-delay value]
```

```
no csna path device
```

Syntax Description		
	<i>path</i>	Hexadecimal value in the range 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the IOCP, the default values for channel logical address and control unit logical address is 0.
	<i>device</i>	Hexadecimal value in the range 00 to FF. This is the unit address associated with the control unit number and path as specified in the host IOCP file.
	<b>maxpiu</b> <i>value</i>	(Optional) Maximum channel I/O block size in bytes that is sent across the physical channel from the CMCC adapter to the attached mainframe. The range is 4096 to 65535 bytes. The default is 20470 bytes.
	<b>time-delay</b> <i>value</i>	(Optional) Number of milliseconds a host-bound SNA frame may be delayed in order to maximize the channel I/O block size. The range is 0 to 100 ms. The default is 10 ms.
	<b>length-delay</b> <i>value</i>	(Optional) Amount of SNA frame data in bytes the CSNA subchannel accumulates before sending the accumulated channel I/O block to the attached mainframe. The range is 0 to 65535 bytes. The default is 20470 bytes.

## show extended channel cmgr

To display information about the MPC+ transmission group (TG) connection manager, use the **show extended channel cmgr** privileged EXEC command.

```
show extended channel slot/port cmgr [tg-name]
```

Syntax Description		
	<i>slot</i>	Slot number.
	<i>port</i>	Physical channel interface port number.
	<i>tg-name</i>	(Optional) Name of the TG.

## show extended channel cmpc

To display information about each CMPC or CMPC+ subchannel configured on the specified channel interface, use the **show extended channel cmpc** privileged EXEC command.

```
show extended channel slot/port cmpc [path [device]]
```

Syntax Description		
	<i>slot</i>	Slot number.
	<i>port</i>	Physical channel interface port number.
	<i>path</i>	(Optional) Logical channel path.
	<i>device</i>	(Optional) 2-digit hexadecimal value that specifies a device address of the CPMC or CMPC+ subchannel. If specified, only status for that CMPC or CMPC+ device is displayed. If not specified, status for all CPMC or CMPC+ devices for the specified path is displayed.

## show extended channel csna

To display information about the CSNA subchannels configured on the specified CMCC interface, use the **show extended channel csna** privileged EXEC command.

```
show extended channel slot/port csna [path [device]] [admin | oper | stats]
```

Syntax Description	
<i>slot</i>	Slot number.
<i>port</i>	Port number.
<i>path</i>	(Optional) A hexadecimal value in the range of 0000 to FFFF. This specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch), one digit for the control unit address, and one digit for the channel logical address. If not specified, information is displayed for all CSNA subchannels configured on the selected interface.
<i>device</i>	(Optional) A hexadecimal value in the range of 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. If not specified, information is displayed for all CSNA subchannels configured with the specified path on the selected interface.
<b>admin</b>	(Optional) Displays configured values for CSNA channel devices. If neither <b>admin</b> , <b>oper</b> , or <b>stats</b> is specified, <b>admin</b> is the default.
<b>oper</b>	(Optional) Displays operational values for CSNA channel devices.
<b>stats</b>	(Optional) Displays statistics for CSNA channel devices.

## show extended channel tg

To display configuration, operational information, and statistics information for CMPC or CMPC+ transmission groups configured on the specified CMCC adapter's virtual interface, use the **show extended channel tg** EXEC command.

```
show extended channel slot/port tg [oper | stats] [detailed] [tg-name]
```

Syntax Description	
<i>slot</i>	Slot number.
<i>port</i>	Port number.
<b>oper</b>	(Optional) Operational parameters for the CMPC or CMPC+ TG values.
<b>stats</b>	(Optional) Statistical values for the CMPC or CMPC+ TG.
<b>detailed</b>	(Optional) Additional information about the CMPC or CMPC+ TG.
<i>tg-name</i>	(Optional) Name of the TG.

## tg (CMPC)

To define LLC connection parameters for the CMPC transmission group, use the **tg** (CMPC) interface configuration command. To remove the specified transmission group from the configuration, which also deactivates the transmission group, use the **no** form of this command.

```
tg name llc token-adapter adapter-number lsap [rmac rmac] [rsap rsap]
```

```
no tg name
```

### Syntax Description

<i>name</i>	Name of the CMPC TG. The maximum length of the name is eight characters. This must match the name specified on the <b>cmpc</b> statements.
<b>llc</b>	Specifies that this TG is connected to the LLC stack on the CMCC adapter card.
<i>token-adapter</i>	Internal adapter type on the CMCC adapter card. The currently supported type is token-adapter.
<i>adapter-number</i>	Internal adapter number on the CMCC adapter card, which is the same value specified in the <b>adapter</b> internal LAN configuration command.
<i>lsap</i>	Local SAP number, 04 to FC, in hexadecimal. The value must be even and should normally be a multiple of four. It must be unique within the internal adapter in that no other IEEE 802.2 clients of that adapter, in the router or in a host, can use the same SAP. The default value is 04.
<b>rmac</b> <i>rmac</i>	(Optional) Remote MAC address of the form <i>xxxx.xxxx.xxxx</i> in hexadecimal. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
<b>rsap</b> <i>rsap</i>	(Optional) Remote SAP address, 04 to FC in hexadecimal. The value for the <i>rsap</i> argument must be even and should be a multiple of 4, but this requirement is not enforced. The default value for the <i>rsap</i> argument is 04.

## tg (CMPC+)

To define IP connection parameters for the CMPC+ transmission group, use the **tg** (CMPC+) interface configuration command. To remove the specified transmission group from the configuration and deactivate the transmission group, use the **no** form of this command.

```
tg tg-name {ip | hsas-ip} host-ip-addr local-ip-addr broadcast
```

```
no tg name
```

**Syntax Description**

<i>tg-name</i>	Name of the CMPC+ TG. The maximum length of the name is eight characters. This name must match the name specified on the <b>cmpc</b> statements.
<b>ip</b>	Specifies that this TG is connected to the TCP/IP stack.
<b>hsas-ip</b>	Specifies that this TG is connected to the HSAS IP stack.
<i>host-ip-addr</i>	Specifies the IP address of the channel-attached host using this TG. A host may have more than one IP stack, therefore this is the IP address of the host IP stack as indicated by the HOME statement in the host TCP/IP profile. For HSAS, this address is the host address as indicated by the <i>source-IP-address</i> parameter of the <b>oeifconfig</b> command.
<i>local-ip-addr</i>	This address must match an IP address configured on the virtual interface. Specifies the IP address of the router to be used for this TG. This is the IP address of the router as indicated by the DEFAULTNET statement in the host TCP/IP profile. For HSAS, this address is the router IP address as indicated by the <i>destination-IP-address</i> parameter of the <b>oeifconfig</b> command.
<b>broadcast</b>	Enables the sending of routing updates to the host.





## TN3270 Server Commands

---

This chapter describes the function and syntax of the commands used to configure and monitor the Cisco Mainframe Channel Connection (CMCC) products, which include the Channel Interface Processor (CIP) and the Channel Port Adapter (CPA). For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*.

### allocate lu

To assign LUs to a pool, use the **allocate lu** listen-point PU configuration command. To remove LUs assigned to a pool, use the **no** form of this command.

**allocate lu** *lu-address* **pool** *poolname* **clusters** *count*

**no allocate lu** *lu-address* **pool** *poolname* **clusters** *count*

Syntax Description		
	<i>lu-address</i>	Starting number of the LOCADDR to which a cluster of LUs are to be allocated.
	<b>pool</b> <i>poolname</i>	Pool name to which you want to allocate LUs. The pool name cannot exceed 8 characters.
	<b>clusters</b> <i>count</i>	Range of LUs in a cluster that are allocated to the specified pool. For example, if the <b>lu</b> keyword specifies the beginning of the LOCADDR number, the <b>cluster</b> keyword specifies the number of clusters to be included in the pool.

### certificate reload

To configure SSL Encryption Support enabled to read the profile security certificate from the file specified in the **servercert** command, use the **certificate reload** profile configuration command.

**certificate reload**

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

## client ip

To add an IP subnet to a client subnet response-time group, use the **client ip** response-time configuration command. To remove an IP subnet from a client subnet response-time group, use the **no** form of this command.

**client ip** *ip-address* [*ip-mask*]

**no client ip** *ip-address* [*ip-mask*]

Syntax Description		
<i>ip-address</i>		IP subnet being added to the response-time group.
<i>ip-mask</i>		(Optional) Mask applied to a client IP address to determine the client's membership in a client subnet group. When the mask is applied to a connecting client's IP address and the resulting address is equal to the defined IP address, the client becomes a member of the client group. The default mask is 255.255.255.255.

## client ip lu

To define a specific LU or range of LUs to a client at the IP address or subnet, use the **client ip lu** TN3270 PU configuration mode command. To cancel this definition, use the **no** form of this command.

**client** [**printer**] **ip** *ip-address* [*ip-mask*] **lu** *first-locaddr* [*last-locaddr*]

**no client** [**printer**] **ip** *ip-address* [*ip-mask*] **lu** *first-locaddr* [*last-locaddr*]

Syntax Description		
<b>printer</b>		(Optional) Specifies that a client connection from the nailed IP addresses will be nailed to one of the specified LUs only if the client-session negotiates a model type of 328 <i>n</i> , where <i>n</i> is any alphanumeric character. Moreover, it ensures that a printer matching the IP address condition can only use an LU nailed as a printer LU.  If the <b>printer</b> keyword is not specified for any <b>client</b> statement that has this IP address set, all model types can use this range of LUs.
<i>ip-address</i>		Specifies remote client IP address.
<i>ip-mask</i>		(Optional) The mask applied to the remote device address. Multiple client IP addresses in the same subnet can be nailed to the same range of locaddrs.
<i>first-locaddr</i>		Defines a single locaddr to nail.
<i>last-locaddr</i>		(Optional) Defines the end range of inclusive locaddrs to be nailed from <i>first-locaddr</i> to <i>last-locaddr</i> .

## client ip pool

To nail clients to pools, use the **client ip pool** listen-point configuration command. To remove clients from pools, use the **no** form of this command.

**client ip** *ip-address* [*ip-mask*] **pool** *poolname*

**no client ip** *ip-address* [*ip-mask*] **pool** *poolname*

Syntax Description		
	<i>ip-address</i>	Remote client IP address.
	<i>ip-mask</i>	(Optional) Mask applied to the remote device address. The mask is part of the matching function that determines whether a client is governed by the nailing statement. The default is 255.255.255.255. Multiple client IP addresses in the same subnet can be nailed to the same range of LOCADDRS.
	<i>poolname</i>	Specifies a unique pool name. The pool name cannot exceed 8 characters.

## client lu maximum

To limit the number of LU sessions that can be established for each client IP address or IP subnet address, use the **client lu maximum** TN3270 server configuration command. To remove a single LU limit associated with a particular IP address, use the **no** form of this command.

**client** [*ip* [*ip-mask*]] **lu maximum** *number*

**no client** [*ip* [*ip-mask*]]

Syntax Description		
	<i>ip</i>	(Optional) IP address of the client. The value for the <i>ip</i> argument is optional when setting the maximum number of LU sessions. If no IP address is specified then the limit is applied to all clients.
	<i>ip-mask</i>	(Optional) IP network mask for the client. The default is 255.255.255.255.
	<i>number</i>	(Optional) Maximum number of LU sessions. The allowed value is from 0 to 65535.

## client pool

To nail clients to pools, use the **client pool** listen-point configuration command. To remove clients from pools, use the **no** form of this command.

**client** {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

**no client** {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

Syntax Description		
<b>ip</b> <i>ip-address</i>		Remote client IP address.
<i>ip-mask</i>		(Optional) Mask applied to the remote device address. The mask is part of the matching function that determines whether a client is governed by the nailing statement. The default is 255.255.255.255. Multiple client IP addresses in the same subnet can be nailed to the same pool.
<b>name</b> <i>DNS-name</i>		(Optional) Alphanumeric string that specifies a client machine name. The string can contain up to 24 characters. If a valid <i>DNS-domain-identifier</i> is not present, this name must be fully qualified. If this name is not fully qualified, any dot that forms the boundary between the DNS-name and the DNS-domain must be included here if it is not already present in the DNS-domain.
<i>DNS-domain-identifier</i>		(Optional) A numeric identifier that specifies a domain name. The valid value range is 1 to 255. Each <b>domain-id</b> command statement can have only one <i>DNS-domain-identifier</i> value.
<b>domain-name</b> <i>DNS-domain</i>		(Optional) Alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain up to 80 characters. All dots must be included when the string is appended to a configured DNS-name. If the DNS-domain starts with a dot, then the dot must be included if it is not already at the end of the DNS-name.
<b>domain-id</b> <i>DNS-domain-identifier</i>		(Optional) Numeric identifier that specifies that a domain name suffix will be appended to the name configured in the domain-id command. The valid value range is 1 to 255. Each <b>domain-id</b> command statement can have only one <i>DNS-domain-identifier</i> value.  The domain-id is originally specified in the <b>domain-id</b> command.
<i>poolname</i>		Specifies a unique pool name. The pool name cannot exceed 8 characters.

## default-profile

To specify the name of the profile to be applied as a default to all the listen points, use the **default-profile** security command. To disable the default profile specification, use the **no** form of this command.

**default-profile** *profilename*

**no default-profile** *profilename*

Syntax Description		
<i>profilename</i>		Profile name should already be configured.

## disable (TN3270)

To turn off security in the TN3270 server, use the **disable** (TN3270) security configuration command.

**disable**

---

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

## dlur

To enable the Systems Network Architecture (SNA) session switch function on the CMCC adapter and enter dependent logical unit requester (DLUR) configuration mode, use the **dlur** TN3270 server configuration command. To disable the SNA session switch function and discard all parameter values associated with the SNA session switch, use the **no** form of this command.

**dlur** [*fq-cpname fq-dlusname*]

**no dlur**

---

<b>Syntax Description</b>	<i>fq-cpname</i>	(Optional) Fully qualified control point (CP) name used by the SNA session switch and the logical unit (LU) name for the DLUR function. This name must be unique among APPN nodes in the network including other values for the <i>fq-cpname</i> argument specified on all other TN3270 servers running under the Cisco IOS software.
	<i>fq-dlusname</i>	(Optional) Fully qualified name of the primary choice for the dependent LU server (DLUS). This is the name of an LU, usually a CP, in an APPN host. The value for the <i>fq-dlusname</i> argument can be repeated and shared across servers.

---

## dlus-backup

To specify a backup DLUS for the DLUR function, use the **dlus-backup** DLUR configuration command. To remove a backup DLUS name, use the **no** form of this command.

**dlus-backup** *dlusname2*

**no dlus-backup**

---

<b>Syntax Description</b>	<i>dlusname2</i>	Fully qualified name of the backup DLUS for the DLUR.
---------------------------	------------------	---

---

## domain-id

To specify a domain name suffix that the TN3270 server appends to a configured machine name to form a fully qualified name when configuring inverse DNS nailing, use the **domain-id** TN3270 server configuration command. To disable this specification, use the **no** form of this command.

**domain-id** *DNS-domain-identifier* *DNS-domain*

**no domain-id** *DNS-domain-identifier* *DNS-domain*

<b>Syntax Description</b>	<i>DNS-domain-identifier</i>	A numeric identifier that specifies the domain name. The valid value range is 1 to 255. Each domain-id statement can have only one <i>DNS-domain-identifier</i> value. This identifier is also used in the <b>client pool</b> command.
	<i>DNS-domain</i>	An alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain no more than 80 characters. All dots must be included when the string is appended to a configured DNS-name. If the DNS-domain starts with a dot, then the dot must be included if it is not already at the end of the DNS-name.

## enable (TN3270)

To turn on security in the TN3270 server, use the **enable** (TN3270) security configuration mode command.

**enable**

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

## encryptorder

To specify the security encryption algorithm for the SSL Encryption Support, use the **encryptorder** profile configuration command.

**encryptorder** [DES] [3DES] [RC4] [RC2] [RC5]

<b>Syntax Description</b>	<b>DES</b>	(Optional) Specifies the DES encryption algorithm.
	<b>3DES</b>	(Optional) Specifies the 3DES encryption algorithm.
	<b>RC4</b>	(Optional) Specifies the RC4 encryption algorithm.
	<b>RC2</b>	(Optional) Specifies the RC2 encryption algorithm.
	<b>RC5</b>	(Optional) Specifies the RC5 encryption algorithm.

## generic-pool

To specify whether or not leftover LUs will be made available to TN3270 sessions that do not request a specific LU or LU pool through TN3270E, use the **generic-pool** TN3270 server configuration command. To selectively remove the permit or deny condition of generic pool use, use the **no** form of this command.

**generic-pool** { **permit** | **deny** }

**no generic-pool**

Syntax Description	permit	deny
	Leftover LUs should be made available to TN3270 users wanting generic sessions. This value is the default.	Leftover LUs should not be given to a generic pool. The physical unit (PU) is not automatically fully populated with 255 LOCADDR definitions. The default is the value configured in TN3270 server configuration mode.

## idle-time

To specify how many seconds of LU inactivity, from both host and client, before the TN3270 session is disconnected, use the **idle-time** TN3270 server configuration command. To cancel the idle time period and return to the default, use the **no** form of this command.

**idle-time** *seconds*

**no idle-time**

Syntax Description	<i>seconds</i>
	Idle time in seconds, from 0 to 65535. A value of 0 means the session is never disconnected.

## ip precedence (TN3270)

To specify the precedence level for voice over IP traffic in the TN3270 server, use the **ip precedence** TN3270 server configuration command. To remove the precedence value, use the **no** form of this command.

**ip precedence** { **screen** | **printer** } *value*

**no ip precedence** { **screen** | **printer** }

Syntax Description	screen	printer	<i>value</i>
	Specifies the precedence is for screen devices.	Specifies the precedence is for printer devices.	Sets the precedence priority. A value between 0 and 7, with 7 being the highest priority. The default is 0.

## ip tos

To specify the Type of Service (ToS) level for IP traffic in the TN3270 server, use the **ip tos** TN3270 server configuration command. To remove the ToS value, use the **no** form of this command.

```
ip tos {screen | printer} value
```

```
no ip tos {screen | printer}
```

Syntax Description		
<b>screen</b>		Specifies the ToS is for screen devices.
<b>printer</b>		Specifies the ToS is for printer devices.
<i>value</i>		Sets the ToS priority. A value between 0 and 15. The default is 0.

## keepalive (TN3270)

To specify how many seconds of inactivity elapse before the TN3270 server transmits a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client, use the **keepalive** TN3270 server configuration command. To cancel the keepalive period and return to the previously configured siftdown value or the default, use the **no** form of this command.

```
keepalive seconds [send {nop | timing-mark [max-response-time]]
```

```
no keepalive
```

Syntax Description		
<i>seconds</i>		Number of elapsed seconds (from 0 to 65535) before the TN3270 server sends a DO TIMING-MARK or Telnet <b>no</b> command to the TN3270 client. A value of 0 means no keepalive signals are sent. The default is 1800 seconds (30 minutes).
<b>send nop</b>		(Optional) Sends the Telnet command for no operation to the TN3270 client to verify the physical connection. No response is required by the client.
<b>send timing-mark</b> [ <i>max-response-time</i> ]		(Optional) Number of seconds (from 0 to 32767) within which the TN3270 server expects a response to the DO TIMING-MARK from the TN3270 client. The default is 30 seconds if the keepalive interval is greater than or equal to 30 seconds. If the value of the keepalive interval is less than 30 seconds, then the default <i>max-response-time</i> is the value of the interval. The value of the <i>max-response-time</i> should be less than or equal to the <i>interval</i> .

## keylen

To specify the maximum bit length for the encryption keys for SSL Encryption Support, use the **keylen 128** profile configuration command. To disable this specification and thereby set the key length to the default of 40 bits, use the **no** form of this command or **keylen 40**.

**keylen** {40 | 128}

**no keylen** [40 | 128]

Syntax Description		
	40	Specifies the bit length for the encryption keys to 40.
	128	Specifies the bit length for the encryption keys to 128.

## link (TN3270)

To define and activate a link to a host, use the **link** DLUR SAP configuration command. To delete the link definition, use the **no** form of this command.

**link** *name* [**r**mac *r*mac] [**r**sap *r*sap]

**no link** *name*

Syntax Description		
	<i>name</i>	Link name, from one to eight alphanumeric characters. The first character must be alphabetic. The name must be unique within the DLUR function.
	<b>r</b> mac <i>r</i> mac	(Optional) Remote MAC address of the form <i>xxxx.xxxx.xxxx</i> in hexadecimal. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
	<b>r</b> sap <i>r</i> sap	(Optional) Remote SAP address, 04 to FC in hexadecimal. The <i>r</i> sap value must be even and should be a multiple of 4, but this requirement is not enforced. The default value for the <i>r</i> sap argument is 04.

## listen-point

To define an IP address for the TN3270 server, use the **listen-point** TN3270 server configuration command. To remove a listen point for the TN3270 server, use the **no** form of this command.

**listen-point** *ip-address* [**t**cp-port *number*]

**no listen-point** *ip-address* [**t**cp-port *number*]

Syntax Description		
	<i>ip-address</i>	IP address that the clients should use as the host IP address to map to LU sessions under this PU and listen point.
	<b>t</b> cp-port <i>number</i>	(Optional) Port number used for the listen operation. The default value is 23.

# Isap

To create a SAP in the SNA session switch and enter DLUR SAP configuration mode, use the **Isap** DLUR configuration command. To delete a SAP and all SNA session switch links using the internal LAN interface, use the **no** form of this command.

**Isap** *type adapter-number [Isap]*

**no Isap** *type adapter-number [Isap]*

Syntax Description		
	<i>type</i>	Internal adapter type on the CIP card, which corresponds to the value specified in the <b>lan</b> internal LAN configuration command. The currently supported value for the <i>type</i> argument is <b>token-adapter</b> .
	<i>adapter-number</i>	Internal adapter interface on the CIP card, which is the same value specified in the <b>adapter</b> internal LAN configuration command.
	<i>Isap</i>	(Optional) Local SAP number, 04 to FC, in hexadecimal. The value must be even and should normally be a multiple of four. It must be unique within the internal adapter in that no other 802.2 clients of that adapter, in the router or in a host, should be allocated the same SAP. The default value is C0.

# lu deletion

To specify whether the TN3270 server sends a REPLY-PSID poweroff request to VTAM to delete the corresponding LU when a client disconnects, use the **lu deletion** TN3270 server configuration command. To remove LU deletion from the current configuration scope, use the **no** form of this command.

**lu deletion** { **always** | **normal** | **non-generic** | **never** | **named** }

**no lu deletion**

Syntax Description		
	<b>always</b>	Always delete dynamic LUs upon disconnect.
	<b>normal</b>	Delete screen LUs only upon disconnect.
	<b>non-generic</b>	Delete only specified LUs upon disconnect.
	<b>never</b>	Never delete LUs upon disconnect.
	<b>named</b>	Delete only named LUs upon disconnect.

## lu termination

To specify whether a TERMSELF or UNBIND RU is sent by the TN3270 server when a client turns off his device or disconnects, use the **lu termination** TN3270 server configuration command. To remove LU termination from the current configuration scope, use the **no** form of this command.

**lu termination** { **termself** | **unbind** }

**no lu termination**

Syntax Description	termself	unbind
	Orders termination of all sessions and session requests associated with an LU upon disconnect.	Requests termination of the session by the application upon LU disconnect. This value is the default.

## maximum-lus

To limit the number of LU control blocks that will be allocated for the TN3270 server, use the **maximum-lus** TN3270 server configuration command. To restore the default value, use the **no** form of this command.

**maximum-lus** *number*

**no maximum-lus**

Syntax Description	<i>number</i>
	Maximum number of LU control blocks allowed. The allowed range is 0 to 32000. However, the practical upper limit for concurrently operating TN3270 sessions depends on the hardware and usage characteristics. The default is 2100.

## pool

To define pool names for the TN3270 server and specify the number of screens and printers in each logical cluster, use the **pool** TN3270 server configuration command. To remove a client IP pool, use the **no** form of this command.

**pool** *poolname* [**cluster layout** *layout-spec-string*]

**no pool** *poolname*

<b>Syntax Description</b>	<i>poolname</i>	Unique pool name which cannot exceed 8 characters. Valid characters are (alphabetic characters are not case sensitive): <ul style="list-style-type: none"> <li>• 1st character—Alphabetic (A-Z) and national characters '@', '#', and '\$'</li> <li>• 2nd-8th characters—Alphabetic (A-Z), numeric (0-9), and national characters '@', '#', and '\$'</li> </ul>
	<b>cluster layout</b> <i>layout-spec-string</i>	(Optional) Name for the cluster and to indicate a cluster of LUs such as printers. The sum of the numbers must be less than or equal to 255. No spaces are used between the entries in the <i>layout-spec-string</i> . The default value is 1a.

## preferred-nnserver

To specify a preferred network node (NN) as server, use the **preferred-nnserver** DLUR configuration command. To remove the preference, use the **no** form of this command.

**preferred-nnserver** *name*

**no preferred-nnserver**

<b>Syntax Description</b>	<i>name</i>	Fully qualified name of an NN.
---------------------------	-------------	--------------------------------

## profile

To specify a name and a security protocol for a security profile and enter profile configuration mode, use the **profile** security configuration command. To remove this name and protocol specification, use the **no** form of this command.

Create a new profile:

**profile** *profilename* {**ssl** | **none**}

Modify an existing profile:

**profile** *profilename*

Delete a profile:

**no profile** *profilename* {**ssl** | **none**}

<b>Syntax Description</b>	<i>profilename</i>	String of alphanumeric characters which specify a name for a security profile. The character range is from 1 to 24. Profile names cannot be duplicated.
	<b>ssl</b>	Specifies that this profile will use the ssl 3.0 security protocol. This implies that the initial exchange between the client and the server is the "Client Hello" message.
	<b>none</b>	Specifies that this profile will not use a security protocol. Sessions using this profile will not use any security.

## pu (DLUR)

To create a PU entity that has no direct link to a host or to enter PU configuration mode, use the **pu** DLUR configuration command. To remove the PU entity, use the **no** form of this command.

```
pu pu-name idblk-idnum ip-address
```

```
no pu pu-name
```

Syntax Description		
	<i>pu-name</i>	Name that uniquely identifies this PU.
	<i>idblk-idnum</i>	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server only enforces uniqueness within the set of DLUR PUs.
	<i>ip-address</i>	IP address that the clients should use as host IP address to map to LU sessions under this PU.

## pu (listen-point)

To create a PU entity that has a direct link to a host or to enter listen-point PU configuration mode, use the **pu** listen-point configuration command. To remove the PU entity, use the **no** form of this command.

```
pu pu-name idblk-idnum type adapter-number lsap [rmac rmac] [rsap rsap]
  [lu-seed lu-name-stem]
```

```
no pu pu-name
```

Syntax Description		
	<i>pu-name</i>	Name that uniquely identifies this PU.
	<i>idblk-idnum</i>	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server cannot tell which remote hosts are in which subareas and does not enforce the unique value requirement.
	<i>type</i>	Internal adapter type on the CIP card, which corresponds to the value specified in the <b>lan</b> internal LAN configuration command. The currently supported type is <b>token-adapter</b> .
	<i>adapter-number</i>	Internal adapter interface on the CIP card, which is the same value specified in the <b>adapter</b> internal LAN configuration command.
	<i>lsap</i>	Local SAP number in hexadecimal, ranging from 04 to DE. The value must be even, and must be unique within the internal adapter so that no other 802.2 clients of that adapter, in the router or in a host, are allocated the same SAP. Other direct links from TN3270 server direct PUs may use the same value on the internal adapter as long as the remote MAC or SAP is different.

<b>rmac</b> <i>rmac</i>	(Optional) Remote MAC address. The remote MAC address in the form <i>xxxx.xxxx.xxxx</i> hexadecimal, specifying the MAC address of the remote host. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
<b>rsap</b> <i>rsap</i>	(Optional) Remote SAP address. The remote SAP address is a one- or two-character hexadecimal string, ranging from 04 to FC, that specifies the SAP address of the remote host. The default is 04.
<b>lu-seed</b> <i>lu-name-stem</i>	(Optional) LU name that the client uses when a specific LU name request is needed. The format is <i>x...x##</i> or <i>x...x###</i> where <i>x...x</i> is an alphanumeric string. When <b>##</b> is specified, it is replaced with the LU LOCADDR in hexadecimal digits to form the complete LU name. When <b>###</b> is specified, decimal digits are used, padded with leading zeroes to make three characters. The first <i>x</i> must be alphabetic and the entire string, including the # symbols, must not exceed 8 characters.

## pu (TN3270)

To create a PU entity that has its own direct link to a host and enter PU configuration mode, use the **pu** TN3270 server configuration command. To remove the PU entity, use the **no** form of this command.

```
pu pu-name idblk-idnum ip-address type adapter-number lsap [rmac rmac] [rsap rsap] [lu-seed
lu-name-stem]
```

```
no pu pu-name
```

### Syntax Description

<i>pu-name</i>	Name that uniquely identifies this PU.
<i>idblk-idnum</i>	The value for this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 Server cannot tell which remote hosts are in which subareas and does not enforce the unique value requirement.
<i>ip-address</i>	IP address that the clients should use as host IP address to map to LU sessions under this PU.
<i>type</i>	Internal adapter type on the CIP card, which corresponds to the value specified in the <b>lan</b> internal LAN configuration command. The currently supported type is <b>token-adapter</b> .
<i>adapter-number</i>	Internal adapter interface on the CIP card, which is the same value specified in the <b>adapter</b> internal LAN configuration command.
<i>lsap</i>	Local SAP number in hexadecimal, ranging from 04 to FC. The value must be even, and must be unique within the internal adapter so that no other 802.2 clients of that adapter, in the router or in a host, should be allocated the same SAP. Other direct links from TN3270 server direct PUs may use the same value on the internal adapter as long as the remote MAC or SAP is different.
<b>rmac</b> <i>rmac</i>	(Optional) Remote MAC address. The remote MAC address of the form <i>xxxx.xxxx.xxxx</i> hexadecimal, specifying the MAC address of the remote host. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.

<b>rsap</b> <i>rsap</i>	(Optional) Remote SAP address. The remote SAP address is a one- or two-character hexadecimal string, ranging from 04 to FC, specifying the SAP address of the remote host. The default is 04.
<b>lu-seed</b> <i>lu-name-stem</i>	(Optional) Provides an LU name that the client can use when a specific LU name request is needed. The format can be <i>x...x##</i> or <i>x...x###</i> where <i>x...x</i> is an alphanumeric string. When <i>##</i> is specified, it is replaced with the LU LOCADDR in hexadecimal digits to form the complete LU name. When <i>###</i> is specified, decimal digits are used, padded with leading zeroes to make three characters. The first <i>x</i> must be alphabetic and the entire string, including the # symbols, must not exceed 8 characters.

## pu dlur (listen-point)

To create a PU entity that has no direct link to a host or to enter listen-point PU configuration mode, use the **pu dlur** listen-point configuration command. To remove the PU entity, use the **no** form of this command.

```
pu pu-name idblk-idnum dlur [lu-seed lu-name-stem]
```

```
no pu pu-name idblk-idnum dlur [lu-seed lu-name-stem]
```

### Syntax Description

<i>pu-name</i>	Name that uniquely identifies this PU.
<i>idblk-idnum</i>	Value for this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server only enforces uniqueness within the set of DLUR PUs.
<b>lu-seed</b> <i>lu-name-stem</i>	<p>(Optional) LU name that the client uses when a specific LU name request is needed. The format is <i>x...x##</i> or <i>x...x###</i> where <i>x...x</i> is an alphanumeric string. When <i>##</i> is specified, it is replaced with the LU LOCADDR in hexadecimal digits to form the complete LU name. When <i>###</i> is specified, decimal digits are used, padded with leading zeroes to make three characters. The first <i>x</i> must be alphabetic (A through Z), or one of the following symbols: \$, #, @. The entire string, including the # symbols, must not exceed 8 characters.</p> <p>The # symbols are allowed in the middle of the lu-seed string. For example, NC##RAL or USA###NC are valid strings. The # symbols cannot be the first characters in the string. For example, ##CISCO is not valid because the first character of the LU name cannot be a number. But ####DOT is valid because the # symbols in the second, third and fourth place are used for LU names. There must be at least two to three consecutive # symbols in the string. For example, SH# or CD#D is not valid. A string without # symbols is not valid. For example, CISCONC is not valid. You must not split the # symbols. For example, SH#NC# and SH#D#NC# are not valid.</p>



**Note** The # sign can signify a value or be used as a symbol.

## response-time group

To configure a client subnet group for response-time measurements, use the **response-time group** TN3270 server configuration command. To remove a client subnet group from response-time measurements, use the **no** form of this command.

**response-time group** *name* [**bucket boundaries** *t1 t2 t3 t4...*] [**multiplier** *m*]

**no response-time group** *name*

<b>Syntax Description</b>	<i>name</i>	Alphanumeric string for the response-time group name. The maximum length of the name is 24 characters. Lower or uppercase letters can be used.
	<b>bucket boundaries</b> <i>t1 t2 t3 t4</i>	(Optional) Unsigned 32-bit quantity that defines a bucket boundary in tenths of seconds. For other types of client groups, the bucket boundaries and multiplier values are fixed to the following defaults: <ul style="list-style-type: none"> <li>• Bucket boundaries—10, 20, 50, 100</li> <li>• Multiplier—30</li> </ul>
	<b>multiplier</b> <i>m</i>	(Optional) Number in the range of 1 to 5760, which when multiplied by the sample interval of 20 seconds, determines the collection interval.

## sec-profile

To specify a security profile to be associated with a listen point, use the **sec-profile** listen-point configuration command. To remove this specification, use the **no** form of this command.

**sec-profile** *profilename*

**no sec-profile** *profilename*

<b>Syntax Description</b>	<i>profilename</i>	Name originally specified in the <b>profile</b> command. It consists of a string of alphanumeric characters that specify the security profile name to be associated with a listen point. The valid character range is from 1 to 24.
---------------------------	--------------------	---

## security (TN3270)

To enable security on the TN3270 server, use the **security** command. To turn off security on the TN3270 server, use the **no** form of this command.

**security**

**no security**

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

## servercert

To specify the location of the TN3270 server's security certificate in the router's Flash memory, use the **servercert** profile configuration command.

**servercert** *location*

### Syntax Description

<i>location</i>	Hexadecimal string of up to 63 characters specifying the location of the server's certificate in the Flash memory.
-----------------	--

## show extended channel tn3270-server

To display current server configuration parameters and the status of the PUs defined for the TN3270 server, use the **show extended channel tn3270-server** EXEC command.

**show extended channel** *slot/port* **tn3270-server**

### Syntax Description

<i>slot</i>	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
<i>port</i>	Port value for a TN3270 server will always be 2.

## show extended channel tn3270-server client-ip-address

To display information about all clients at a specific IP address, use the **show extended channel tn3270-server client-ip-address** EXEC command.

**show extended channel** *slot/port* **tn3270-server client-ip-address** *ip-address* [**disconnected** | **in-session** | **pending**]

### Syntax Description

<i>slot</i>	Slot number.
<i>port</i>	Port number.
<i>ip-address</i>	IP address of the client.
<b>disconnected</b>	(Optional) Displays all clients with <i>ip-address</i> in disconnected state. Disconnected state refers to an LU session state of ACTIVE or INACTIVE. In this case, the <i>ip-address</i> refers to the client that last used the LU.
<b>in-session</b>	(Optional) Displays all clients with <i>ip-address</i> in active session state. Active session state refers to an LU session state of ACT/SESS.
<b>pending</b>	(Optional) Displays all clients with <i>ip-address</i> in pending state. Pending session state refers to an LU session state of P-SDT, P-ACTLU, P-NTF/AV, P-NTF/UA, P-RESET, P-PSID, P-BIND, P-UNBIND, WT-UNBND, WT-SDT or UNKNOWN.

## show extended channel tn3270-server client-name

To display information about all connected clients with a specific machine name, use the **show extended channel tn3270-server client-name** EXEC command.

```
show extended channel slot/virtual channel tn3270-server client-name name
```

Syntax Description	slot	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
	<i>virtual channel</i>	Virtual channel number.
	<i>name</i>	Specifies the client machine name. This name is specified originally in the <b>client pool</b> command.

## show extended channel tn3270-server dlur

To display information about the SNA session switch, use the **show extended channel tn3270-server dlur** EXEC command.

```
show extended channel slot/port tn3270-server dlur
```

Syntax Description	slot	Slot number.
	<i>port</i>	Port number.

## show extended channel tn3270-server dlurlink

To display information about the DLUR components, use the **show extended channel tn3270-server dlurlink** EXEC command.

```
show extended channel slot/port tn3270-server dlurlink name
```

Syntax Description	slot	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
	<i>port</i>	Port number.
	<i>name</i>	Name of the SNA session switch link to be displayed.

## show extended channel tn3270-server nailed-domain

To list all nailing statements with a specific nailed-domain name, use the **show extended channel tn3270-server nailed-domain** EXEC command.

```
show extended channel slot/virtual channel tn3270-server nailed-domain name
```

Syntax Description		
<i>slot</i>		Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
<i>virtual channel</i>		Virtual channel number.
<i>name</i>		Specifies the <i>exact</i> nailed-domain name, as specified originally in the <b>client pool</b> command. Output is displayed for the nailed-domain name <i>exactly</i> as specified. That is, specifying “cisco.com” is different from specifying “.ciosco.com.”

## show extended channel tn3270-server nailed-ip

To display mappings between a nailed client IP address and nailed LUs, use the **show extended channel tn3270-server nailed-ip** EXEC command.

```
show extended channel slot/port tn3270-server nailed-ip ip-address
```

Syntax Description		
<i>slot</i>		Slot number.
<i>port</i>		Port number.
<i>ip-address</i>		Remote client IP address.

## show extended channel tn3270-server nailed-name

To list all nailing statements with a specific nailed machine name, use the **show extended channel tn3270-server nailed-name** EXEC command.

```
show extended channel slot/virtual channel tn3270-server nailed-name name
```

Syntax Description		
<i>slot</i>		Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
<i>virtual channel</i>		Virtual channel number.
<i>name</i>		Specifies the nailed machine name. This name is specified originally in the <b>client pool</b> command.

## show extended channel tn3270-server pu

To display configuration parameters for a PU and all the LUs currently attached to the PU, including the LU cluster layout and pool name, use the **show extended channel tn3270-server pu** EXEC command.

```
show extended channel slot/virtual channel tn3270-server pu pu-name [cluster | client-name]
```

Syntax Description		
<i>slot</i>		Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
<i>virtual channel</i>		Virtual channel number.
<i>pu-name</i>		Name that uniquely identifies this PU.

<b>cluster</b>	(Optional) Displays cluster information for the LUs within the pool.
<b>client-name</b>	(Optional) Displays client name information for the LUs within the pool.

## show extended channel tn3270-server pu lu

To display information about the TN3270 server LUs running on CMCC adapter interface, use the **show extended channel tn3270-server pu lu** EXEC command.

```
show extended channel slot/port tn3270-server pu pu-name lu locaddr [history]
```

### Syntax Description

<i>slot</i>	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number. The port value for a TN3270 server will always be 2.
<i>port</i>	Port value for a TN3270 server will always be 2.
<i>pu-name</i>	PU name that uniquely identifies this PU.
<i>locaddr</i>	LU LOCADDR that uniquely identifies the LU.
<b>history</b>	(Optional) Displays the LU trace history.

## show extended channel tn3270-server response-time application

To display information for application client groups, use the **show extended channel tn3270-server response-time application** privileged EXEC command.

```
show extended channel slot/virtual channel tn3270-server response-time application
[appl-name [detail]]
```

### Syntax Description

<i>slot</i>	Slot number.
<i>virtual channel</i>	Virtual channel number.
<i>appl-name</i>	(Optional) Display only the client group corresponding to the VTAM application name.
<b>detail</b>	(Optional) List client members and their response-time statistics following the client group entry.

## show extended channel tn3270-server response-time global

To display information about the global client group, use the **show extended channel tn3270-server response-time global** privileged EXEC command.

```
show extended channel slot/virtual channel tn3270-server response-time global
```

**Syntax Description**

<i>slot</i>	Slot number.
<i>virtual channel</i>	Virtual channel number.

## show extended channel tn3270-server response-time link

To display information about host link client groups, use the **show extended channel tn3270-server response-time link** privileged EXEC command.

```
show extended channel slot/virtual channel tn3270-server response-time link [link-name]
```

**Syntax Description**

<i>slot</i>	Slot number.
<i>virtual channel</i>	Port number.
<i>link-name</i>	(Optional) PU name for a direct PU or link name for a DLUR PU.

## show extended channel tn3270-server response-time listen-point

To display information about listen point client groups, use the **show extended channel tn3270-server response-time listen-point** privileged EXEC command.

```
show extended channel slot/virtual channel tn3270-server response-time listen-point
```

**Syntax Description**

<i>slot</i>	Slot number.
<i>virtual channel</i>	Virtual channel number.

## show extended channel tn3270-server response-time subnet

To display information about Subnet client groups, use the **show extended channel tn3270-server response-time subnet** privileged EXEC command.

```
show extended channel slot/virtual channel tn3270-server response-time subnet [ip-address
ip-mask [detail]]
```

**Syntax Description**

<i>slot</i>	Slot number.
<i>virtual channel</i>	Virtual channel number.
<b>ip-address</b>	(Optional) Subnet IP address.
<i>ip-mask</i>	(Optional) Subnet mask.
<b>detail</b>	(Optional) Each client group entry is followed by a list of its client members and their respective response-time statistics.

## show extended channel tn3270-server security

To display information about the TN3270 security enhancement, use the **show extended channel tn3270-server security** EXEC command.

```
show extended channel slot/virtual channel tn3270-server security [[sec-profile profilename]
[listen-point ipaddress [tcp-port number]]]
```

Syntax Description		
<i>slot</i>		Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
<i>virtual channel</i>		Virtual channel number.
<b>sec-profile</b> <i>profilename</i>	(Optional)	Alphanumeric name which specifies the security profile name to be associated with a listen point. The character range is from 1 to 24. This name is specified originally in the <b>profile</b> command.
<b>listen-point</b> <i>ipaddress</i>	(Optional)	IP address that the clients should use as the host IP address to map to LU sessions under this PU and listen point.
<b>tcp-port</b> <i>number</i>	(Optional)	Port number used for the listen operation. The default value is 23.

## shutdown (TN3270)

To shut down TN3270 entities, such as PU, DLUR, and DLUR SAP, use the **shutdown** command in one of the TN3270 server command modes. The **shutdown** TN3270 command shuts down the TN3270 entities according to which configuration mode you are in when the command is issued. To restart the interface or entity, use the **no** form of this command.

**shutdown**

**no shutdown**

Syntax Description	
	This command has no arguments or keywords.

## tcp-port

To override the default TCP port setting of 23, use the **tcp-port** TN3270 server configuration command. To restore the default, use the **no** form of this command.

**tcp-port** *port-number*

**no tcp-port**

Syntax Description		
<i>port-number</i>		A valid TCP port number in the range of 0 to 65534. The default is 23, which is the IETF standard. The value 65535 is reserved by the TN3270 server.

## timing-mark

To select whether a WILL TIMING-MARK is transmitted when the host application needs an SNA response (definite or pacing response), use the **timing-mark** TN3270 server configuration command. To turn off WILL TIMING-MARK transmission except as used by the keepalive function, use the **no** form of this command.

**timing-mark**

**no timing-mark**

---

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

## tn3270-server

To start the TN3270 server on a CMCC adapter or to enter TN3270 server configuration mode, use the **tn3270-server** interface configuration command. To remove the existing TN3270 server configuration, use the **no** form of this command.

**tn3270-server**

**no tn3270-server**

---

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

## unbind-action

To select what action to take when the TN3270 server receives an UNBIND request, use the **unbind-action** TN3270 server configuration command. To restore the default, use the **no** form of this command.

**unbind-action {keep | disconnect}**

**no unbind-action**

---

<b>Syntax Description</b>	<b>keep</b>	No automatic disconnect will be made by the server on receipt of an UNBIND.
	<b>disconnect</b>	Session will be disconnected upon receipt of an UNBIND.

---

## **vrn**

To tell the SNA session switch the connection network to which the internal adapter interface on the CMCC adapter belongs, use the **vrn** DLUR SAP configuration command. To remove a network name, use the **no** form of this command.

**vrn** *vrn-name*

**no vrn**

---

**Syntax Description**

---

*vrn-name*

---

Fully qualified name of the connection network.

---



## **Quality of Service Solutions**





## Quality of Service Commands: **access-list rate-limit** Through **match ip dscp**

---

This chapter describes the function and syntax of the quality of service (QoS) commands: **access-list rate-limit** through **match ip dscp**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Quality of Service Solutions 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. Value values are from 0 to 7.
<b>mask mask</b>	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.

---

## bandwidth (policy-map-class)

To specify or modify the bandwidth allocated for a class belonging to a policy map, use the **bandwidth** policy-map class configuration command. To remove the bandwidth specified for a class, use the **no** form of this command.

**bandwidth** { *bandwidth-kbps* | **percent** *percent* }

**no bandwidth** { *bandwidth-kbps* | **percent** *percent* }

### Syntax Description

<i>bandwidth-kbps</i>	Amount of bandwidth, in kbps, to be assigned to the class.
<b>percent</b> <i>percent</i>	Percentage of available bandwidth to be assigned to the class.

## bgp-policy

To enable the Policy Propagation via Border Gateway Protocol (BGP) feature on the interface, use the **bgp-policy** interface configuration command. To disable the Policy Propagation via BGP feature, use the **no** form of this command.

**bgp-policy ip-prec-map**

**no bgp-policy ip-prec-map**

### Syntax Description

<b>ip-prec-map</b>	QoS policy based on the IP Precedence.
--------------------	--

## bump

To configure the bumping rules for a virtual circuit (VC) class that can be assigned to a VC bundle, use the **bump** vc-class configuration command. To remove the explicit bumping rules for the VCs assigned this class and default them to implicit bumping, use the **no bump explicit** command. To specify that the VC bundle members do not accept any bumped traffic, use the **no bump traffic** command.

To configure the bumping rules for a specific VC member of a bundle, use the **bump** bundle-vc configuration command. To remove the explicit bumping rules for the VC and default it to implicit bumping, use the **no bump explicit** command. To specify that the VC does not accept any bumped traffic, use the **no** form of this command.

**bump** { **implicit** | **explicit** *precedence-level* | **traffic** }

**no bump** { **explicit** *precedence-level* | **traffic** }

<b>Syntax Description</b>	<b>implicit</b>	Depending on the mode, applies implicit bumping rules, which is also the default, to a single VC bundle member (bundle-vc mode) or all VCs in the bundle (bundle mode). The (default) implicit bumping rule stipulates that bumped traffic is to be carried by a VC with a lower precedence.
	<b>explicit</b> <i>precedence-level</i>	Specifies the precedence level to which traffic on a VC (bundle-vc mode) will be bumped when the VC goes down. Specifies a single number as the value of the <i>precedence-level</i> argument.
	<b>traffic</b>	In its positive form, specifies that the VC accepts bumped traffic. The <b>no</b> form stipulates that the VC does not accept any bumped traffic.

## bundle

To create a bundle or modify an existing bundle to enter bundle configuration mode, use the **bundle** subinterface configuration command. To remove the specified bundle, use the **no** form of this command.

**bundle** *bundle-name*

**no bundle** *bundle-name*

<b>Syntax Description</b>	<i>bundle-name</i>	Specifies the name of the bundle to be created. Limit is 16 alphanumeric characters.
---------------------------	--------------------	--

## class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class** policy-map configuration command. To remove a class from the policy map, use the **no** form of this command.

**class** { *class-name* | **class-default** }

**no class** { *class-name* | **class-default** }

<b>Syntax Description</b>	<i>class-name</i>	The name of the class for which you want to configure or modify policy.
	<b>class-default</b>	Specifies the default class so that you can configure or modify its policy.

## class-bundle

To configure a virtual circuit (VC) bundle with the bundle-level commands contained in the specified VC class, use the **class-bundle** bundle configuration command. To remove the VC class parameters from a VC bundle, use the **no** form of this command.

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

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

---

### Syntax Description

---

<i>vc-class-name</i>	Name of the VC class you are assigning to your VC bundle.
----------------------	---

---

## class-map

To create a class map to be used for matching packets to a specified class, use the **class-map** global configuration command. To remove an existing class map from the router, use the **no** form of this command.

**class-map** *class-map-name*

**no class-map** *class-map-name*

---

### Syntax Description

---

<i>class-map-name</i>	Name of the class for the class map. The class name is used for both the class map and to configure policy for the class in the policy map.
-----------------------	---

---

## custom-queue-list

To assign a custom queue list to an interface, use the **custom-queue-list** interface configuration command. To remove a specific list or all list assignments, use the **no** form of this command.

**custom-queue-list** [*list-number*]

**no custom-queue-list** [*list-number*]

---

### Syntax Description

---

<i>list-number</i>	Any number from 1 to 16 for the custom queue list.
--------------------	--

---

## disconnect qdm

To disconnect a Quality of Service Device Manager (QDM) client, use the **disconnect qdm** EXEC command.

**disconnect qdm** [**client** *client-id*]

<b>Syntax Description</b>	<b>client</b>	(Optional) Specifies that a specific QDM client will be disconnected.
	<i>client-id</i>	(Optional) Specifies the specific QDM identification number to disconnect.

## dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **dscp** command in `cfg-red-grp` configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

```
dscp dscpvalue min-threshold max-threshold [mark-probability-denominator]
```

```
no dscp dscpvalue min-threshold max-threshold [mark-probability-denominator]
```

<b>Syntax Description</b>	<i>dscpvalue</i>	Specifies the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: <b>ef</b> , <b>af11</b> , <b>af12</b> , <b>af13</b> , <b>af21</b> , <b>af22</b> , <b>af23</b> , <b>af31</b> , <b>af32</b> , <b>af33</b> , <b>af41</b> , <b>af42</b> , <b>af43</b> , <b>cs1</b> , <b>cs2</b> , <b>cs3</b> , <b>cs4</b> , <b>cs5</b> , or <b>cs7</b> .
	<i>min-threshold</i>	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drops some packets with the specified DSCP value.
	<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value.
	<i>mark-probability-denominator</i>	(Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; one out of every ten packets is dropped at the maximum threshold.

## exponential-weighting-constant

To configure the exponential weight factor for the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group, use the **exponential-weighting-constant** `random-detect-group` configuration command. To return the exponential weight factor for the group to the default, use the **no** form of this command.

```
exponential-weighting-constant exponent
```

```
no exponential-weighting-constant
```

<b>Syntax Description</b>	<i>exponent</i>	Exponent from 1 to 16 used in the average queue size calculation.
---------------------------	-----------------	---

## fair-queue (class-default)

To specify the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy, use the **fair-queue** policy-map class configuration command. To delete the configured number of dynamic queues from the class-default policy, use the **no** form of this command.

**fair-queue** [*number-of-dynamic-queues*]

**no fair-queue** [*number-of-dynamic-queues*]

---

### Syntax Description

*number-of-dynamic-queues* (Optional) A power of 2 number in the range from 16 to 4096 specifying the number of dynamic queues.

---

## fair-queue (DWFQ)

To enable VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue** interface configuration command. The command enables DWFQ on an interface using a VIP2-40 or greater interface processor. To disable DWFQ, use the **no** form of this command.

**fair-queue**

**no fair-queue**

---

### Syntax Description

This command has no arguments or keywords.

## fair-queue (policy-map)

To specify the number of queues to be reserved for use by a traffic class, use the **fair-queue** policy-map configuration command. To delete the configured number of queues from the traffic class, use the **no** form of this command.

**fair-queue** [**queue-limit** *queue-value*]

**no fair-queue** [**queue-limit** *queue-value*]

---

### Syntax Description

**queue-limit** (Optional) A keyword used to specify or modify the maximum number of packets that a per-flow queue can hold.

*queue-value* (Optional) A number specifying the maximum number of packets that each per-flow queue can accumulate.

---

## fair-queue (WFQ)

To enable weighted fair queueing (WFQ) for an interface, use the **fair-queue** interface configuration command. To disable WFQ for an interface, use the **no** form of this command.

**fair-queue** [*congestive-discard-threshold* [*dynamic-queues* [*reservable-queues*]]]

**no fair-queue**

Syntax Description	
<i>congestive-discard-threshold</i>	(Optional) Number of messages allowed in each queue. The default is 64 messages, and a new threshold must be a power of 2 in the range from 16 to 4096. When a conversation reaches this threshold, new message packets are discarded.
<i>dynamic-queues</i>	(Optional) Number of dynamic queues used for best-effort conversations (that is, a normal conversation not requiring any special network services). Values are <b>16, 32, 64, 128, 256, 512, 1024, 2048, and 4096</b> . See Table 4 and Table 5 in the <b>fair-queue</b> (class-default) command for the default number of dynamic queues.
<i>reservable-queues</i>	(Optional) Number of reservable queues used for reserved conversations in the range 0 to 1000. The default is 0. Reservable queues are used for interfaces configured for features such as Resource Reservation Protocol (RSVP).

## fair-queue aggregate-limit

To set the maximum number of packets in all queues combined for VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue aggregate-limit** interface configuration command. To return the value to the default, use the **no** form of this command.

**fair-queue aggregate-limit** *aggregate-packets*

**no fair-queue aggregate-limit**

Syntax Description	
<i>aggregate-packets</i>	Total number of buffered packets allowed before some packets may be dropped. Below this limit, packets will not be dropped.

## fair-queue individual-limit

To set the maximum individual queue depth for VIP-distributed weighted fair queuing (DWFQ), use the **fair-queue individual-limit** interface configuration command. To return the value to the default, use the **no** form of this command.

**fair-queue individual-limit** *individual-packet*

**no fair-queue individual-limit**

### Syntax Description

<i>individual-packet</i>	Maximum number of packets allowed in each per-flow or per-class queue during periods of congestion.
--------------------------	---

## fair-queue limit

To set the maximum queue depth for a specific VIP-distributed weighted fair queuing (DWFQ) class, use the **fair-queue limit** interface configuration command. To return the value to the default, use the **no** form of this command.

**fair-queue** {**qos-group** *number* | **tos** *number*} **limit** *class-packet*

**no fair-queue** {**qos-group** *number* | **tos** *number*} **limit** *class-packet*

### Syntax Description

<b>qos-group</b> <i>number</i>	Number of the QoS group, as assigned by a committed access rate (CAR) policy or the Policy Propagation via Border Gateway Protocol (BGP) feature. The value can range from 1 to 99.
<b>tos</b> <i>number</i>	Two low-order IP Precedence bits of the type of service (ToS) field.
<i>class-packet</i>	Maximum number of packets allowed in the queue for the class during periods of congestion.

## fair-queue qos-group

To enable VIP-distributed weighted fair queuing (DWFQ) and classify packets based on the internal QoS-group number, use the **fair-queue qos-group** interface configuration command. To disable QoS-group-based DWFQ, use the **no** form of this command.

**fair-queue qos-group**

**no fair-queue qos-group**

### Syntax Description

This command has no arguments or keywords.

## fair-queue tos

To enable VIP-distributed weighted fair queueing (DWFQ) and classify packets using the type of service (ToS) field of packets, use the **fair-queue tos** interface configuration command. To disable ToS-based DWFQ, use the **no** form of this command.

**fair-queue tos**

**no fair-queue tos**

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

## fair-queue weight

To assign a weight to a class for VIP-distributed weighted fair queueing (DWFQ), use the **fair-queue weight** interface configuration command. To remove the bandwidth allocated for the class, use the **no** form of this command.

**fair-queue { qos-group *number* | tos *number* } weight *weight***

**no fair-queue { qos-group *number* | tos *number* } weight *weight***

<b>Syntax Description</b>	<b>qos-group <i>number</i></b>	Number of the QoS group, as assigned by a committed access rate (CAR) policy or the Policy Propagation via Border Gateway Protocol (BGP) feature. The value range is from 1 to 99.
	<b>tos <i>number</i></b>	Two low-order IP Precedence bits of the type of service (ToS) field. The value range is from 1 to 3.
	<b><i>weight</i></b>	Percentage of the output link bandwidth allocated to this class. The sum of weights for all classes cannot exceed 99.

## frame-relay interface-queue priority

To enable the Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature, use the **frame-relay interface-queue priority** interface configuration command. To disable FR PIPQ, use the **no** form of this command.

**frame-relay interface-queue priority [*high-limit medium-limit normal-limit low-limit*]**

**no frame-relay interface-queue priority**

To assign priority to a permanent virtual circuit (PVC) within a Frame Relay map class, use the **frame-relay interface-queue priority** map-class configuration command. To remove priority from a PVC within a Frame Relay map class, use the **no** form of this command.

**frame-relay interface-queue priority { **high** | **medium** | **normal** | **low** }**

**no frame-relay interface-queue priority**

<b>Syntax Description</b>	<i>high-limit</i>	(Optional) Size of the high priority queue specified in maximum number of packets.
	<i>medium-limit</i>	(Optional) Size of the medium priority queue specified in maximum number of packets.
	<i>normal-limit</i>	(Optional) Size of the normal priority queue specified in maximum number of packets.
	<i>low-limit</i>	(Optional) Size of the low priority queue specified in maximum number of packets.
	<b>high</b>	Assigns high priority to a PVC.
	<b>medium</b>	Assigns medium priority to a PVC.
	<b>normal</b>	Assigns normal priority to a PVC.
	<b>low</b>	Assigns low priority to a PVC.

## frame-relay ip rtp priority

To reserve a strict priority queue on a Frame Relay permanent virtual circuit (PVC) for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **frame-relay ip rtp priority** map-class configuration command. To disable the strict priority queue, use the **no** form of this command.

**frame-relay ip rtp priority** *starting-rtp-port-number port-number-range bandwidth*

**no frame-relay ip rtp priority**

<b>Syntax Description</b>	<i>starting-rtp-port-number</i>	The starting UDP port number. The lowest port number to which the packets are sent.
	<i>port-number-range</i>	The range of UDP destination ports. Number, which added to the <i>starting-rtp-port-number</i> argument, yields the highest UDP port number.
	<i>bandwidth</i>	Maximum allowed bandwidth, in kbps.

## ip nbar pdlm

To extend or enhance the list of protocols recognized by Network-Based Application Recognition (NBAR) through a Cisco-provided Packet Description Language Module (PDLM), use the **ip nbar pdlm** global configuration command. To unload a PDLM if it was previously loaded, use the **no** form of this command.

**ip nbar pdlm** *pdlm-name*

**no ip nbar pdlm** *pdlm-name*

<b>Syntax Description</b>	<i>pdlm-name</i>	The URL where the PDLM can be found on the Flash card.
---------------------------	------------------	--

## ip nbar port-map

To configure Network-Based Application Recognition (NBAR) to search for a protocol or protocol name using a port number other than the well-known port, use the **ip nbar port-map** global configuration command. To look for the protocol name using only the well-known port number, use the **no** form of this command.

```
ip nbar port-map protocol-name [tcp | udp] port-number
```

```
no ip nbar port-map protocol-name [tcp | udp] port-number
```

<b>Syntax Description</b>	<i>protocol-name</i>	Name of protocol known to NBAR.
<b>tcp</b>		(Optional) Specifies that a TCP port will be searched for the specified <i>protocol-name</i> argument.
<b>udp</b>		(Optional) Specifies that a UDP port will be searched for the specified <i>protocol-name</i> argument.
<i>port-number</i>		Assigned port for named protocol. The <i>port-number</i> argument is either a UDP or a TCP port number, depending on which protocol is specified in this command line. Up to 16 <i>port-number</i> arguments can be specified in one command line.

## ip nbar protocol-discovery

To configure Networked-Based Application Recognition (NBAR) to discover traffic for all protocols known to NBAR on a particular interface, use the **ip nbar protocol-discovery** interface configuration command. To disable traffic discovery, use the **no** form of this command.

```
ip nbar protocol-discovery
```

```
no ip nbar protocol-discovery
```

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

## ip rsvp atm-peak-rate-limit

To set a limit on the peak cell rate (PCR) of reservations for all newly created Resource Reservation Protocol (RSVP) switched virtual circuits (SVCs) established on the current interface or any of its subinterfaces, use the **ip rsvp atm-peak-rate-limit** interface configuration command. To remove the current peak rate limit, in which case the reservation peak rate is limited by the line rate, use the **no** form of this command.

```
ip rsvp atm-peak-rate-limit limit
```

```
no ip rsvp atm-peak-rate-limit
```

<b>Syntax Description</b>	<i>limit</i>	The peak rate limit of the reservation specified, in KB. The minimum value allowed is 1 KB; the maximum value allowed is 2 GB.
---------------------------	--------------	--

## ip rsvp bandwidth

To enable Resource Reservation Protocol (RSVP) for IP on an interface, use the **ip rsvp bandwidth** interface configuration command. To disable RSVP, use the **no** form of this command.

```
ip rsvp bandwidth [interface-kbps [single-flow-kbps]]
```

```
no ip rsvp bandwidth [interface-kbps [single-flow-kbps]]
```

<b>Syntax Description</b>	<i>interface-kbps</i>	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated by RSVP flows. The range is from 1 to 10,000,000.
	<i>single-flow-kbps</i>	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range is from 1 to 10,000,000.

## ip rsvp burst policing

To configure a burst factor within the Resource Reservation Protocol (RSVP) token bucket policer on a per-interface basis, use the **ip rsvp burst policing** interface configuration command. To return to the default value, enter the **no** form of this command.

```
ip rsvp burst policing [factor]
```

```
no ip rsvp burst policing
```

<b>Syntax Description</b>	<i>factor</i>	(Optional) Indicates a burst factor value as a percentage of the requested burst of the receiver.
---------------------------	---------------	---

## ip rsvp dsbm candidate

To configure an interface as a Designated Subnetwork Bandwidth Manager (DSBM) candidate, use the **ip rsvp dsbm candidate** interface configuration command. To disable DSBM on an interface, which exempts the interface as a DSBM candidate, use the **no** form of this command.

```
ip rsvp dsbm candidate [priority]
```

```
no ip rsvp dsbm candidate
```

### Syntax Description

<i>priority</i>	(Optional) A value in the range from 64 to 128. Among contenders for the DSBM, the interface with the highest priority number wins the DSBM election process.
-----------------	---

## ip rsvp dsbm non-resv-send-limit

To configure the NonResvSendLimit object parameters, use the **ip rsvp dsbm non-resv-send-limit** interface configuration command. To use the default NonResvSendLimit object parameters, use the **no** form of this command.

```
ip rsvp dsbm non-resv-send-limit {rate kbps | burst kilobytes | peak kbps | min-unit bytes |  
max-unit bytes}
```

```
no ip rsvp dsbm non-resv-send-limit {rate kbps | burst kilobytes | peak kbps | min-unit bytes |  
max-unit bytes}
```

### Syntax Description

<i>rate kbps</i>	The average rate, in kbps, for the Designated Subnetwork Bandwidth Manager (DSBM) candidate.
<i>burst kilobytes</i>	The maximum burst size, in KB, for the DSBM candidate.
<i>peak kbps</i>	The peak rate, in kbps, for the DSBM candidate.
<i>min-unit bytes</i>	The minimum policed unit, in bytes, for the DSBM candidate.
<i>max-unit bytes</i>	The maximum packet size, in bytes, for the DSBM candidate.

## ip rsvp flow-assist

To enable Resource Reservation Protocol (RSVP) to attach itself to NetFlow so that it can leverage NetFlow services to obtain flow classification information about packets in order to update its token bucket and set IP Precedence as required, use the **ip rsvp flow-assist** interface configuration command. To detach RSVP from NetFlow, use the **no** form of this command.

**ip rsvp flow-assist**

**no ip rsvp flow-assist**

---

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

## ip rsvp neighbor

To enable neighbors to request a reservation, use the **ip rsvp neighbor** interface configuration command. To disable this feature, use the **no** form of this command.

**ip rsvp neighbor** *access-list-number*

**no ip rsvp neighbor** *access-list-number*

---

**Syntax Description** *access-list-number* Number of a standard or extended access list. It can be any number in the range from 1 to 199.

---

## ip rsvp policy cops minimal

To lower the load of the COPS server and to improve latency times for messages on the governed router, use the **ip rsvp policy cops minimal** global configuration command to restrict the COPS RSVP policy to adjudicate only PATH and RESV messages. To turn off the restriction, use the **no** form of this command.

**ip rsvp policy cops minimal**

**no ip rsvp policy cops minimal**

---

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

## ip rsvp policy cops report-all

To enable a router to report on its success and failure with outsourcing decisions, use the **ip rsvp policy cops report-all** global configuration command. To return the router to its default, use the **no** form of this command.

**ip rsvp policy cops report-all**

**no ip rsvp policy cops report-all**

---

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

## ip rsvp policy cops servers

To specify that Resource Reservation Protocol (RSVP) should use Common Open Policy Service (COPS) policy for remote adjudication, use the **ip rsvp policy cops servers** global configuration command. To turn off the use of COPS for RSVP, use the **no** form of this command.

**ip rsvp policy cops** [*acl*] **servers** *server-ip* [*server-ip*]

**no ip rsvp policy cops** [*acl*] **servers**

---

<b>Syntax Description</b>	<i>acl</i>	(Optional) Specifies the access control list (ACL) whose sessions will be governed by the COPS policy.
	<i>server-ip</i>	Specifies the IP addresses of the servers governing the COPS policy. As many as eight servers can be specified, with the first being treated as the primary server.

---

## ip rsvp policy cops timeout

To configure the amount of time the Policy Enforcement Point (PEP) router will retain policy information after losing connection with the Common Open Policy Service (COPS) server, use the **ip rsvp policy cops timeout** global configuration command. To restore the router to the default value (5 minutes), use the **no** form of this command.

**ip rsvp policy cops timeout** *policy-timeout*

**no ip rsvp policy cops timeout**

---

<b>Syntax Description</b>	<i>policy-timeout</i>	Duration of timeout, from 1 to 10,000 seconds.
---------------------------	-----------------------	--

---

## ip rsvp policy default-reject

To reject all messages that do not match the policy access control lists (ACLs), use the **ip rsvp policy default-reject** global configuration command. To restore the default behavior, which passes along all messages that do not match the ACLs, use the **no** form of this command.

**ip rsvp policy default-reject**

**no ip rsvp policy default-reject**

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

## ip rsvp pq-profile

To specify the criteria for Resource Reservation Protocol (RSVP) to use to determine which flows to direct into the priority queue (PQ) within weighted fair queueing (WFQ), use the **ip rsvp pq-profile** global configuration command. To disable the specified criteria, use the **no** form of this command.

**ip rsvp pq-profile** [*voice-like* | *r'* [*b'* [*p-to-r'* | *ignore-peak-value*]]]

**no ip rsvp pq-profile**

<b>Syntax Description</b>	<i>voice-like</i>	(Optional) Indicates pq-profile parameters sufficient for most voice flows. The default values for <i>r'</i> , <i>b'</i> , and <i>p-to-r'</i> are used. These values should cause all voice flows generated from Cisco IOS applications and most voice flows from other RSVP applications, such as Microsoft NetMeeting, to be directed into the PQ.
	<i>r'</i>	(Optional) Indicates maximum rate of a flow in bytes per second. Valid range is from 1 to 1048576 bytes per second.
	<i>b'</i>	(Optional) Indicates maximum burst of a flow in bytes. Valid range is from 1 to 8192 bytes.
	<i>p-to-r'</i>	(Optional) Indicates maximum ratio of peak rate to average rate as a percentage. Valid range is from 100 to 4000 percent.
	<i>ignore-peak-value</i>	(Optional) Indicates that the peak rate to average rate ratio of the flow is not evaluated when RSVP identifies flows.

## ip rsvp precedence

To enable the router to mark the IP Precedence value of the type of service (ToS) byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for packets that either conform to or exceed the RSVP flowspec, use the **ip rsvp precedence** interface configuration command. To remove existing IP Precedence settings, use the **no** form of this command; if neither the **conform** nor **exceed** keyword is specified, all IP Precedence settings are removed.

```
ip rsvp precedence [conform precedence-value] [exceed precedence-value]
```

```
no ip rsvp precedence [conform] [exceed]
```

Syntax Description	
<b>conform</b> <i>precedence-value</i>	(Optional) Specifies an IP Precedence value in the range from 0 to 7 for traffic that conforms to the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the <b>conform</b> or <b>exceed</b> keyword is required; both keywords may be specified.  When used with the <b>no</b> form of the command, the <b>conform</b> keyword is optional.
<b>exceed</b> <i>precedence-value</i>	(Optional) Specifies an IP Precedence value in the range from 0 to 7 for traffic that exceeds the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the <b>conform</b> or <b>exceed</b> keyword is required; both keywords may be specified.  When used with the <b>no</b> form of the command, the <b>exceed</b> keyword is optional.

## ip rsvp reservation

To enable a router to simulate receiving and forwarding Resource Reservation Protocol (RSVP) RESV messages, use the **ip rsvp reservation** global configuration command. To disable this feature, use the **no** form of this command.

```
ip rsvp reservation session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport  
sender-sport next-hop-ip-address next-hop-interface {ff | se | wf} {rate | load} bandwidth  
burst-size
```

```
no ip rsvp reservation session-ip-address sender-ip-address {tcp | udp | ip-protocol}  
session-dport sender-sport next-hop-ip-address next-hop-interface {ff | se | wf} {rate | load}  
bandwidth burst-size
```

Syntax Description	
<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, this is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender.
<b>tcp</b>   <b>udp</b>   <i>ip-protocol</i>	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 255.

<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for <b>wf</b> reservations, for which the source port is always ignored and can therefore be zero).
<i>next-hop-ip-address</i>	Host name or address of the receiver or the router closest to the receiver.
<i>next-hop-interface</i>	Next hop interface or subinterface type and number. Interface type can be <b>ethernet</b> , <b>loopback</b> , <b>null</b> , or <b>serial</b> .
<b>ff</b>   <b>se</b>   <b>wf</b>	Reservation style: <ul style="list-style-type: none"> <li>Fixed Filter (<b>ff</b>) is single reservation.</li> <li>Shared Explicit (<b>se</b>) is shared reservation, limited scope.</li> <li>Wild Card Filter (<b>wf</b>) is shared reservation, unlimited scope.</li> </ul>
<b>rate</b>   <b>load</b>	QoS guaranteed bit rate service or controlled load service.
<i>bandwidth</i>	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

## ip rsvp reservation-host

To enable a router to simulate a host generating Resource Reservation Protocol (RSVP) RESV messages, use the **ip rsvp reservation-host** global configuration command. To disable this feature, use the **no** form of this command.

```
ip rsvp reservation-host session-ip-address sender-ip-address {tcp | udp | ip-protocol}
session-dport sender-sport {ff | se | wf} {rate | load} bandwidth burst-size
```

```
no ip rsvp reservation-host session-ip-address sender-ip-address {tcp | udp | ip-protocol}
session-dport sender-sport {ff | se | wf} {rate | load} bandwidth burst-size
```

### Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver. IP multicast addresses cannot be used with this argument. It must be a logical address configured on an interface on the router you are configuring.
<i>sender-ip-address</i>	The IP address of the sender.
<b>tcp</b>   <b>udp</b>   <i>ip-protocol</i>	TCP, User Datagram Protocol UDP, or IP protocol in the range from 0 to 255.
<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for <b>wf</b> reservations, for which the source port is always ignored and can therefore be zero).

<b>ff   se   wf</b>	Reservation style: <ul style="list-style-type: none"> <li>• Fixed Filter (<b>ff</b>) is single reservation.</li> <li>• Shared Explicit (<b>se</b>) is shared reservation, limited scope.</li> <li>• Wild Card Filter (<b>wf</b>) is shared reservation, unlimited scope.</li> </ul>
<b>rate   load</b>	QoS guaranteed bit rate service or controlled load service.
<i>bandwidth</i>	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

## ip rsvp sender

To enable a router to simulate receiving and forwarding Resource Reservation Protocol (RSVP) PATH messages, use the **ip rsvp sender** global configuration command. To disable this feature, use the **no** form of this command.

```
ip rsvp sender session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport
sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size
```

```
no ip rsvp sender session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport
sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size
```

### Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender.
<b>tcp   udp   ip-protocol</b>	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 255.
<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for <b>wf</b> reservations, for which the source port is always ignored and can therefore be zero).
<i>previous-hop-ip-address</i>	Address of the sender or the router closest to the sender.
<i>previous-hop-interface</i>	Address of the previous hop interface or subinterface. Interface type can be <b>ethernet</b> , <b>loopback</b> , <b>null</b> , or <b>serial</b> .
<i>bandwidth</i>	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

## ip rsvp sender-host

To enable a router to simulate a host generating a Resource Reservation Protocol (RSVP) PATH message, use the **ip rsvp sender-host** global configuration command. To disable this feature, use the **no** form of this command.

```
ip rsvp sender-host session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport sender-sport bandwidth burst-size
```

```
no ip rsvp sender-host session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport sender-sport bandwidth burst-size
```

### Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender. It must be a logical address configured on an interface on the router you are configuring.
<b>tcp</b>   <b>udp</b>   <i>ip-protocol</i>	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 255.
<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for <b>wf</b> reservations, for which the source port is always ignored and can therefore be zero).
<i>bandwidth</i>	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

## ip rsvp signalling dscp

To specify the DSCP to be used on all RSVP messages transmitted on an interface, use the **ip rsvp signalling dscp** interface configuration command. To disable the **ip rsvp signalling dscp** interface configuration command, use the **no** form of this command.

```
ip rsvp signalling dscp [value]
```

```
no ip rsvp signalling dscp
```

### Syntax Description

<i>value</i>	Indicates a number from 0 to 63.
--------------	----------------------------------

## ip rsvp svc-required

To enable creation of a switched virtual circuit (SVC) to service any new Resource Reservation Protocol (RSVP) reservation made on the interface or subinterface of an Enhanced ATM port adapter (PA-A3), use the **ip rsvp svc-required** interface configuration command. To disable SVC creation for RSVP reservations, use the **no** form of this command.

```
ip rsvp svc-required
```

```
no ip rsvp svc-required
```

### Syntax Description

This command has no arguments or keywords.

## ip rsvp tos

To enable the router to mark the five low-order type of service (ToS) bits of the IP header ToS byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for traffic that either conforms to or exceeds the RSVP flowspec, use the **ip rsvp tos** interface configuration command. To remove existing settings for the ToS bits, use the **no** form of this command; if neither the **conform** nor **exceed** keyword is specified, all settings for the ToS bits are removed.

```
ip rsvp tos [[conform tos-value] [exceed tos-value]]
```

```
no ip rsvp tos [conform] [exceed]
```

### Syntax Description

<b>conform</b> <i>tos-value</i>	(Optional) Specifies a ToS value in the range from 0 to 31 for traffic that conforms to the RSVP flowspec. The ToS value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the <b>conform</b> or <b>exceed</b> keyword is required; both keywords may be specified.  When used with the <b>no</b> form of the command, the <b>conform</b> keyword is optional.
<b>exceed</b> <i>tos-value</i>	(Optional) Specifies a ToS value in the range from 0 to 31 for traffic that exceeds the RSVP flowspec. The ToS byte value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the <b>conform</b> or <b>exceed</b> keyword is required; both keywords may be specified.  When used with the <b>no</b> form of the command, the <b>exceed</b> keyword is optional.

## ip rsvp udp-multicasts

To instruct the router to generate User Datagram Protocol (UDP)-encapsulated Resource Reservation Protocol (RSVP) multicasts whenever it generates an IP-encapsulated multicast packet, use the **ip rsvp udp-multicasts** interface configuration command. To disable this feature, use the **no** form of this command.

**ip rsvp udp-multicasts** [*multicast-address*]

**no ip rsvp udp-multicasts** [*multicast-address*]

### Syntax Description

*multicast-address* (Optional) Host name or UDP multicast address of router.

## ip rtp priority

To reserve a strict priority 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 priority** interface configuration command. To disable the strict priority queue, use the **no** form of this command.

**ip rtp priority** *starting-rtp-port-number port-number-range bandwidth*

**no ip rtp priority**

### Syntax Description

<i>starting-rtp-port-number</i>	The starting RTP port number. The lowest port number to which the packets are sent.
<i>port-number-range</i>	The range of UDP destination ports. Number, when added to the <i>starting-rtp-port-number</i> argument, that yields the highest UDP port number.
<i>bandwidth</i>	Maximum allowed bandwidth, in kbps.

## match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** class-map configuration command. To remove ACL match criteria from a class map, use the **no** form of this command.

**match access-group** {*access-group* | **name** *access-group-name*}

**no match access-group** *access-group*

**Syntax Description**

<i>access-group</i>	A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class.
<b>name</b> <i>access-group-name</i>	A named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class.

## match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **match any** class-map configuration command. To remove all criteria as successful match criteria, use the **no** form of this command.

**match any**

**no match any**

**Syntax Description**

This command has no arguments or keywords.

## match class-map

To use a traffic class as a classification policy, use the **match class-map** class-map configuration command. To remove a specific traffic class as a match criterion, use the **no** form of this command.

**match class-map** *class-map-name*

**no match class-map** *class-map-name*

**Syntax Description**

<i>class-map-name</i>	Specifies the name of the traffic class to use as a match criterion.
-----------------------	--

## match cos

To match a packet based on a Layer 2 class of service (CoS) marking, use the **match cos** command in class-map configuration mode. To remove a specific Layer 2 CoS/Inter-Switch Link (ISL) marking, use the **no** form of this command:

**match cos** *cos-value* [*cos-value cos-value cos-value*]

**no match cos** *cos-value* [*cos-value cos-value cos-value*]

**Syntax Description**

<i>cos-value</i>	(Optional) Specific IEEE 802.1Q/ISL CoS value. The <i>cos-value</i> is from 0 to 7; up to four CoS values can be specified in one <b>match cos</b> statement.
------------------	---

## match destination-address mac

To use the destination MAC address as a match criterion, use the **match destination-address mac** class-map configuration command. To remove a previously specified destination MAC address as a match criterion, use the **no** form of this command.

**match destination-address mac** *address*

**no match destination-address mac** *address*

<b>Syntax Description</b>	<i>address</i>	Specifies the specific destination MAC address to be used as a match criterion.
---------------------------	----------------	---

## match input-interface

To configure a class map to use the specified input interface as a match criterion, use the **match input-interface** class-map configuration command. To remove the input interface match criterion from a class map, use the **no** form of this command.

**match input-interface** *interface-name*

**no match input-interface** *interface-name*

<b>Syntax Description</b>	<i>interface-name</i>	Name of the input interface to be used as match criteria.
---------------------------	-----------------------	---

## match ip dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match ip dscp** class-map configuration command. To remove a specific IP DSCP value from a class map, use the **no** form of this command.

**match ip dscp** *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

**no match ip dscp** *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

<b>Syntax Description</b>	<i>ip-dscp-value</i>	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.
---------------------------	----------------------	---



## Quality of Service Commands: match ip precedence Through set qos-group

---

This chapter describes the function and syntax of the quality of service (QoS) commands: **match ip precedence** through **set qos-group**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Quality of Service Solutions Command Reference*.

### match ip precedence

To identify IP precedence values as match criteria, use the **match ip precedence** command in class-map configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

```
match ip precedence ip-precedence-value [ip-precedence-value ip-precedence-value ip-precedence-value]
```

```
no match ip precedence ip-precedence value [ip-precedence-value ip-precedence-value ip-precedence-value]
```

<b>Syntax Description</b>	<i>ip-precedence-value</i>	Specifies the exact value from 0 to 7 used to identify an IP precedence value.
---------------------------	----------------------------	--

### match ip rtp

To configure a class map to use the Real-Time Protocol (RTP) protocol port as the match criterion, use the **match ip rtp** class-map configuration command. To remove the RTP protocol port match criterion, use the **no** form of this command.

```
match ip rtp starting-port-number port-range
```

```
no match ip rtp
```

<b>Syntax Description</b>	<i>starting-port-number</i>	The starting RTP port number. Values range from 2000 to 65535.
	<i>port-range</i>	The RTP port number range. Values range from 0 to 16383.

## match mpls experimental

To configure a class map to use the specified value of the EXP field as a match criterion, use the **match mpls experimental** class-map configuration command. To remove the EXP field match criterion from a class map, use the **no** form of this command.

**match mpls experimental** *number*

**no match mpls experimental** *number*

---

### Syntax Description

*number*

The EXP field value to be used as match criteria. Any number from 0 to 7.

---

## match not

To specify the single match criterion value to use as an unsuccessful match criterion, use the **match not** class-map configuration command. To remove a previously specified source value to not use as a match criterion, use the **no** form of this command.

**match not** *match-criteria*

**no match not** *match-criteria*

---

### Syntax Description

*match-criteria*

(Required) Specifies the match criterion value that is an unsuccessful match criterion. All other values of the specified match criterion will be considered successful match criteria.

---

## match protocol

To configure the match criteria for a class map on the basis of the specified protocol, use the **match protocol** class-map configuration command. To remove protocol-based match criteria from a class map, use the **no** form of this command.

**match protocol** *protocol-name*

**no match protocol** *protocol-name*

Syntax Description	<i>protocol-name</i>	Name of the protocol used as a matching criterion. The following protocols are supported:
		<ul style="list-style-type: none"> <li>• <b>aarp</b>—AppleTalk Address Resolution Protocol</li> <li>• <b>apollo</b>—Apollo Domain</li> <li>• <b>arp</b>—IP Address Resolution Protocol (ARP)</li> <li>• <b>bridge</b>—bridging</li> <li>• <b>bstun</b>—Block Serial Tunneling</li> <li>• <b>cdp</b>—Cisco Discovery Protocol</li> <li>• <b>clns</b>—ISO Connectionless Network Service</li> <li>• <b>clns_es</b>—ISO CLNS End System</li> <li>• <b>clns_is</b>—ISO CLNS Intermediate System</li> <li>• <b>cmns</b>—ISO Connection-Mode Network Service</li> <li>• <b>compressedtcp</b>—compressed TCP</li> <li>• <b>decnet</b>—DECnet</li> <li>• <b>decnet_node</b>—DECnet Node</li> <li>• <b>decnet_router-I1</b>—DECnet Router L1</li> <li>• <b>decnet_router-I2</b>—DECnet Router L2</li> <li>• <b>dlsw</b>—data-link switching</li> <li>• <b>ip</b>—IP</li> <li>• <b>ipx</b>—Novell IPX</li> <li>• <b>llc2</b>—llc2</li> <li>• <b>pad</b>—packet assembler/disassembler links</li> <li>• <b>qllc</b>—Qualified Logical Link Control protocol</li> <li>• <b>rsrb</b>—remote source-route bridging</li> <li>• <b>snapshot</b>—snapshot routing support</li> <li>• <b>stun</b>—serial tunnel</li> <li>• <b>vines</b>—Banyan VINES</li> <li>• <b>xns</b>—Xerox Network Services</li> </ul>

## match protocol citrix

To configure Network-Based Application Recognition (NBAR) to match Citrix traffic, use the **match protocol citrix** class-map configuration command. To disable NBAR from matching Citrix traffic, use the **no** form of this command.

```
match protocol citrix [app application-name-string]
```

```
no match protocol citrix [app application-name-string]
```

Syntax Description		
	<b>app</b>	(Optional) Specifies matching of an application name string.
	<i>application-name-string</i>	(Optional) Specifies string to be used as the subprotocol parameter.

## match protocol http

To configure Network-Based Application Recognition (NBAR) to match Hypertext Transfer Protocol (HTTP) traffic by URL, HOST, or Multipurpose Internet Mail Extension (MIME)-type, use the **match protocol http** class-map configuration command. To disable NBAR from matching HTTP traffic by URL, HOST, or MIME-type, use the **no** form of this command.

```
match protocol http [url url-string | host hostname-string | mime MIME-type]
```

```
no match protocol http [url url-string | host hostname-string | mime MIME-type]
```

Syntax Description		
	<b>url</b>	(Optional) Specifies matching by a URL.
	<i>url-string</i>	(Optional) User-specified URL of HTTP traffic to be matched.
	<b>host</b>	(Optional) Specifies matching by a host name.
	<i>hostname-string</i>	(Optional) User-specified host name to be matched.
	<b>mime</b>	(Optional) Specifies matching by MIME text string.
	<i>MIME-type</i>	(Optional) User-specified MIME text string to be matched.

## match qos-group

To identify a specific QoS group value as a match criterion, use the **match qos-group** command in class-map configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

```
match qos-group qos-group-value
```

```
no match qos-group qos-group-value
```

Syntax Description		
	<i>qos-group-value</i>	Specifies the exact value from 0 to 99 used to identify a QoS group value.

## match source-address mac

To use the source MAC address as a match criterion, use the **match source-address mac** class-map configuration command. To remove a previously specified source MAC address as a match criterion in class map configuration mode, use the **no** form of this command.

**match source-address mac** *address-destination*

**no match source-address mac** *address-destination*

<b>Syntax Description</b>	<i>address-destination</i>	Specifies the source destination MAC address to be used as a match criterion.
---------------------------	----------------------------	---

## max-reserved-bandwidth

To change the percent of interface bandwidth allocated for Resource Reservation Protocol (RSVP), class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PVC Interface Priority Queueing (PIPQ), use the **max-reserved bandwidth** interface configuration command. To restore the default value, use the **no** form of this command.

**max-reserved-bandwidth** *percent*

**no max-reserved-bandwidth**

<b>Syntax Description</b>	<i>percent</i>	Percent of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ.
---------------------------	----------------	--

## oam-bundle

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for a virtual circuit (VC) class that can be applied to a VC bundle, use the **oam-bundle** vc-class configuration command. To remove OAM management from the class configuration, use the **no** form of this command.

To enable end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, use the **oam-bundle** bundle configuration command. To remove OAM management from the bundle, use the **no** form of this command.

**oam-bundle** [**manage**] [*frequency*]

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

<b>Syntax Description</b>	<b>manage</b>	(Optional) Enables OAM management. If this keyword is omitted, loopback cells are sent but the bundle is not managed.
	<i>frequency</i>	(Optional) Number of seconds between sending OAM loopback cells. Values range from 0 to 600 seconds.

# police

To configure the Traffic Policing feature, use the **police** policy-map configuration command. To remove the Traffic Policing feature from the configuration, use the **no** form of this command.

**police** *bps burst-normal burst-max conform-action action exceed-action action* [**violate-action action**]

**no police** *bps burst-normal burst-max conform-action action exceed-action action* [**violate-action action**]

## Syntax Description

<i>bps</i>	Average rate, in bits per second.
<i>burst-normal</i>	Normal burst size, in bytes.
<i>burst-max</i>	Excess burst size, in bytes. In Cisco IOS Release 12.1(5)T onward, the excess burst-size need not be specified unless the <b>violate-action</b> option is also specified. In Cisco IOS Releases 12.0(5)XE through 12.1(1)E, the excess burst size must be specified.
<b>conform-action</b>	Action to take on packets that conform to the rate limit.
<b>exceed-action</b>	Action to take on packets that exceed the rate limit.
<b>violate-action</b>	(Optional) Action to take on packets that violate the normal and maximum burst sizes. If the <b>violate-action</b> option is specified, the token bucket algorithm works with two token buckets.
	This option is not available in Cisco IOS Release 12.0 XE or Release 12.1 E.
<i>action</i>	Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> <li>• <b>drop</b>—Drops the packet.</li> <li>• <b>set-prec-transmit</b> <i>new-prec</i>—Sets the IP precedence and sends the packet.</li> <li>• <b>set-qos-transmit</b> <i>new-qos</i>—Sets the QoS group and sends the packet.</li> <li>• <b>set-dscp-transmit</b>—Sets the differentiated services code point (DSCP) value and transmits the packet.</li> <li>• <b>transmit</b>—Sends the packet.</li> </ul>

# policy-map

To create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** global configuration command. To delete a policy map, use the **no** form of this command.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

## Syntax Description

<i>policy-map-name</i>	Name of the policy map.
------------------------	-------------------------

## precedence (VC bundle)

To configure precedence levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **precedence** vc-class configuration command. To remove the precedence levels from the VC class, use the **no** form of this command.

To configure the precedence levels for a VC member of a bundle, use the **precedence** bundle-vc configuration command. To remove the precedence levels from the VC, use the **no** form of this command.

**precedence** [*other* | *range*]

**no precedence**

Syntax Description		
	<b>other</b>	(Optional) Any precedence levels in the range from 0 to 7 that are not explicitly configured.
	<i>range</i>	(Optional) A single precedence level specified as a number, or a range of precedence levels, specified as a hyphenated range.

## precedence (WRED group)

To configure a Weighted Random Early Detection (WRED) or VIP-distributed WRED (DWRED) group for a particular IP Precedence, use the **precedence** random-detect-group configuration command. To return the values for each IP Precedence for the group to the default values, use the **no** form of this command.

**precedence** *precedence min-threshold max-threshold mark-probability-denominator*

**no precedence** *precedence min-threshold max-threshold mark-probability-denominator*

Syntax Description		
	<i>precedence</i>	IP Precedence number. Values range from 0 to 7.
	<i>min-threshold</i>	Minimum threshold in number of packets. Value range from 1 to 4096. When the average queue length reaches this number, WRED or DWRED begins to drop packets with the specified IP Precedence.
	<i>max-threshold</i>	Maximum threshold in number of packets. The value range is <i>min-threshold</i> to 4096. When the average queue length exceeds this number, WRED or DWRED drops all packets with the specified IP Precedence.
	<i>mark-probability-denominator</i>	Denominator for the fraction of packets dropped when the average queue depth is <i>max-threshold</i> . For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the <i>max-threshold</i> . The value is 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the <i>max-threshold</i> .

## priority

To give priority to a class of traffic belonging to a policy map, use the **priority** policy-map class configuration command. To remove a previously specified priority specified for a class, use the **no** form of this command.

```
priority { bandwidth-kbps | percent percentage } [burst]
```

```
no priority { bandwidth-kbps | percent percentage } [burst]
```

### Syntax Description

<i>bandwidth-kbps</i>	Guaranteed allowed bandwidth, in kbps, for the priority traffic. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved.
<b>percent</b>	Specifies that the amount of guaranteed bandwidth will be specified by the percent of available bandwidth.
<i>percentage</i>	Used in conjunction with the <b>percent</b> keyword, specifies the percentage of the total available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100.
<i>burst</i>	(Optional) Specifies the burst size, in bytes. The range of the burst is 32 to 2,000,000 bytes.

## priority-group

To assign the specified priority list to an interface, use the **priority-group** interface configuration command. To remove the specified priority group assignment, use the **no** form of this command.

```
priority-group list-number
```

```
no priority-group list-number
```

### Syntax Description

<i>list-number</i>	Priority list number assigned to the interface. Any number from 1 to 16.
--------------------	--

## priority-list default

To assign a priority queue for those packets that do not match any other rule in the priority list, use the **priority-list default** global configuration command. To return to the default or assign **normal** as the default, use the **no** form of this command.

```
priority-list list-number default { high | medium | normal | low }
```

```
no priority-list list-number default
```

### Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b>	Priority queue level. The <b>normal</b> queue is used if you use the <b>no</b> form of this command.

## priority-list interface

To establish queueing priorities on packets entering from a given interface, use the **priority-list interface** global configuration command. To remove an entry from the list, use the **no** form of this command with the appropriate arguments.

```
priority-list list-number interface interface-type interface-number {high | medium | normal | low}
```

```
no priority-list list-number interface interface-type interface-number {high | medium | normal | low}
```

### Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>interface-type</i>	The type of the interface.
<i>interface-number</i>	The number of the interface.
<b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b>	Priority queue level.

## priority-list protocol

To establish queueing priorities based upon the protocol type, use the **priority-list protocol** global configuration command. To remove a priority list entry assigned by protocol type, use the **no** form of this command with the appropriate arguments.

```
priority-list list-number protocol protocol-name {high | medium | normal | low} queue-keyword keyword-value
```

```
no priority-list list-number protocol [protocol-name {high | medium | normal | low} queue-keyword keyword-value]
```

### Syntax Description

<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>protocol-name</i>	Protocol type: <b>aarp</b> , <b>apollo</b> , <b>appletalk</b> , <b>arp</b> , <b>bridge</b> (transparent), <b>clns</b> , <b>clns_es</b> , <b>clns_is</b> , <b>compressedtcp</b> , <b>cmns</b> , <b>decnet</b> , <b>decnet_node</b> , <b>decnet_router-l1</b> , <b>decnet_router-l2</b> , <b>dls</b> , <b>ip</b> , <b>ipx</b> , <b>pad</b> , <b>rsrb</b> , <b>stun</b> , <b>vines</b> , <b>xns</b> , and <b>x25</b> .
<b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b>	Priority queue level.
<i>queue-keyword</i> <i>keyword-value</i>	Possible keywords are <b>fragments</b> , <b>gt</b> , <b>list</b> , <b>lt</b> , <b>tcp</b> , and <b>udp</b> .

## priority-list queue-limit

To specify the maximum number of packets that can be waiting in each of the priority queues, use the **priority-list queue-limit** global configuration command. To select the normal queue, use the **no** form of this command.

**priority-list** *list-number* **queue-limit** [*high-limit* [*medium-limit* [*normal-limit* [*low-limit*]]]]

**no priority-list** *list-number* **queue-limit**

Syntax Description	
<i>list-number</i>	Any number from 1 to 16 that identifies the priority list.
<i>high-limit</i>	(Optional) Priority queue maximum length. A value of 0 for any of the four
<i>medium-limit</i>	arguments means that the queue can be of unlimited size for that particular queue.
<i>normal-limit</i>	For default values for these arguments, see Table 13.
<i>low-limit</i>	

## protect

To configure a virtual circuit (VC) class with protected group or protected VC status for application to a VC bundle member, use the **protect** command in vc-class configuration mode. To remove the protected status from the VC class, use the **no** form of this command.

To configure a specific VC as part of a protected group of the bundle or to configure it as an individually protected VC bundle member, use the **protect** command in bundle-vc configuration mode. To remove the protected status from the VC, use the **no** form of this command.

**protect** {*group* | *vc*}

**no protect** {*group* | *vc*}

Syntax Description	
<b>group</b>	Configures the VC bundle member as part of the protected group of the bundle.
<b>vc</b>	Configures the VC member as individually protected.

## pvc-bundle

To add a virtual circuit (VC) to a bundle as a member of the bundle and enter bundle-vc configuration mode in order to configure that VC bundle member, use the **pvc-bundle** bundle configuration command. To remove the VC from the bundle, use the **no** form of this command.

**pvc-bundle** *pvc-name* [*vpi/*] [*vci*]

**no pvc-bundle** *pvc-name* [*vpi/*] [*vci*]

**Syntax Description**

<i>pvc-name</i>	The name of the permanent virtual circuit (PVC) bundle.
<i>vpi</i>	<p>(Optional) 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, the value range is from 0 to 255; on the Cisco 4500 and 4700 routers, the value range is from 0 to 1 less than the quotient of 8192 divided by the value set by the <b>atm vc-per-vp</b> command.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p>
<i>vci</i>	<p>(Optional) ATM network virtual channel identifier (VCI) for this PVC. The value range is from 0 to 1 less than the maximum value set for this interface by the <b>atm vc-per-vp</b> command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signalling, Integrated Local Management Interface (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 <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p>

## qos pre-classify

To enable QoS preclassification, use the **qos pre-classify** interface configuration command. To disable the QoS preclassification feature, use the **no** form of this command.

```
qos pre-classify
```

```
no qos pre-classify
```

**Syntax Description**

This command has no arguments or keywords.

## queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** policy-map class configuration command. To remove the queue packet limit from a class, use the **no** form of this command.

```
queue-limit number-of-packets
```

```
no queue-limit number-of-packets
```

**Syntax Description**

<i>number-of-packets</i>	A number in the range from 1 to 64 specifying the maximum number of packets that the queue for this class can accumulate.
--------------------------	---

## queue-list default

To assign a priority queue for those packets that do not match any other rule in the queue list, use the **queue-list default** global configuration command. To restore the default value, use the **no** form of this command.

**queue-list** *list-number* **default** *queue-number*

**no queue-list** *list-number* **default** *queue-number*

### Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.

## queue-list interface

To establish queueing priorities on packets entering on an interface, use the **queue-list interface** global configuration command. To remove an entry from the list, use the **no** form of this command.

**queue-list** *list-number* **interface** *interface-type* *interface-number* *queue-number*

**no queue-list** *list-number* **interface** *interface-type* *interface-number* *queue-number*

### Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16 that identifies the queue list.
<i>interface-type</i>	Type of the interface.
<i>interface-number</i>	Number of the interface.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.

## queue-list protocol

To establish queueing priority based upon the protocol type, use the **queue-list protocol** global configuration command. To remove an entry from the list, use the **no** form of this command.

**queue-list** *list-number* **protocol** *protocol-name* *queue-number* *queue-keyword* *keyword-value*

**no queue-list** *list-number* **protocol** *protocol-name* *queue-number* *queue-keyword* *keyword-value*

### Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16.
<i>protocol-name</i>	Protocol type: <b>aarp</b> , <b>apollo</b> , <b>appletalk</b> , <b>arp</b> , <b>bridge</b> (transparent), <b>clns</b> , <b>clns_es</b> , <b>clns_is</b> , <b>cmns</b> , <b>compressedtcp</b> , <b>decnet</b> , <b>decnet_node</b> , <b>decnet_router11</b> , <b>decnet_router12</b> , <b>dls</b> , <b>ip</b> , <b>ipx</b> , <b>pad</b> , <b>rsrb</b> , <b>stun</b> , <b>vines</b> , <b>xns</b> , and <b>x25</b> .
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.
<i>queue-keyword</i> <i>keyword-value</i>	Possible keywords are <b>fragments</b> , <b>gt</b> , <b>list</b> , <b>lt</b> , <b>tcp</b> , and <b>udp</b> .

## queue-list queue byte-count

To specify how many bytes the system allows to be delivered from a given queue during a particular cycle, use the **queue-list queue byte-count** global configuration command. To return the byte count to the default value, use the **no** form of this command.

**queue-list** *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

**no queue-list** *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

### Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.
<i>byte-count-number</i>	The average number of bytes the system allows to be delivered from a given queue during a particular cycle.

## queue-list queue limit

To designate the queue length limit for a queue, use the **queue-list queue limit** global configuration command. To return the queue length to the default value, use the **no** form of this command.

**queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*

**no queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*

### Syntax Description

<i>list-number</i>	Number of the queue list. Any number from 1 to 16.
<i>queue-number</i>	Number of the queue. Any number from 1 to 16.
<i>limit-number</i>	Maximum number of packets that can be enqueued at any time. The range is from 0 to 32767 queue entries. A value of 0 means that the queue can be of unlimited size.

## random-detect dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **random-detect dscp** interface configuration command. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

**random-detect dscp** *dscpvalue* *min-threshold* *max-threshold* [*mark-probability-denominator*]

**no random-detect dscp** *dscpvalue* *min-threshold* *max-threshold* [*mark-probability-denominator*]

Syntax Description		
	<i>dscpvalue</i>	Specifies the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: <b>ef</b> , <b>af11</b> , <b>af12</b> , <b>af13</b> , <b>af21</b> , <b>af22</b> , <b>af23</b> , <b>af31</b> , <b>af32</b> , <b>af33</b> , <b>af41</b> , <b>af42</b> , <b>af43</b> , <b>cs1</b> , <b>cs2</b> , <b>cs3</b> , <b>cs4</b> , <b>cs5</b> , or <b>cs7</b> .
	<i>min-threshold</i>	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drops some packets with the specified DSCP value.
	<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value.
	<i>mark-probability-denominator</i>	(Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

## random-detect (interface)

To enable Weighted Random Early Detection (WRED) or distributed WRED (DWRED), use the **random-detect** interface configuration command. To configure WRED as class policy in a policy map, use the **random-detect** interface and policy-map class configuration command. To disable WRED or DWRED, use the **no** form of this command.

```
random-detect [dscp-based | prec-based]
```

```
no random-detect [dscp-based | prec-based]
```

Syntax Description		
	<i>dscp-based</i>	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
	<i>prec-based</i>	(Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.

## random-detect (per VC)

To enable per-virtual circuit (VC) Weighted Random Early Detection (WRED) or per-VC VIP-distributed WRED (DWRED), use the **random-detect** VC submode command. To disable per-VC WRED and per-VC DWRED, use the **no** form of this command.

```
random-detect [attach group-name]
```

```
no random-detect [attach group-name]
```

---

**Syntax Description**

**attach** *group-name* (Optional) The name of the WRED or DWRED group.

---

## random-detect exponential-weighting-constant

To configure the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) exponential weight factor for the average queue size calculation for the queue, use the **random-detect exponential-weighting-constant** interface configuration command. To configure the exponential weight factor for the average queue size calculation for the queue reserved for a class, use the **random-detect exponential-weighting-constant** policy-map class configuration command. To return the value to the default, use the **no** form of this command.

```
random-detect exponential-weighting-constant exponent
```

```
no random-detect exponential-weighting-constant
```

---

**Syntax Description**

*exponent* Exponent from 1 to 16 used in the average queue size calculation.

---

## random-detect flow

To enable flow-based Weighted Random Early Detection (WRED), use the **random-detect flow** interface configuration command. To disable flow-based WRED, use the **no** form of this command.

```
random-detect flow
```

```
no random-detect flow
```

---

**Syntax Description**

This command has no arguments or keywords.

## random-detect flow average-depth-factor

To set the multiplier to be used in determining the average depth factor for a flow when flow-based Weighted Random Early Detection (WRED) is enabled, use the **random-detect flow average-depth-factor** interface configuration command. To remove the current flow average depth factor value, use the **no** form of this command.

**random-detect flow average-depth-factor** *scaling-factor*

**no random-detect flow average-depth-factor** *scaling-factor*

<b>Syntax Description</b>	<i>scaling-factor</i>	The numbers 2, 4, 8, or 16.
---------------------------	-----------------------	-----------------------------

## random-detect flow count

To set the flow count for flow-based Weighted Random Early Detection (WRED), use the **random-detect flow count** interface configuration command. To remove the current flow count value, use the **no** form of this command.

**random-detect flow count** *number*

**no random-detect flow count** *number*

<b>Syntax Description</b>	<i>number</i>	Specifies a value from 16 to 2 <sup>15</sup> (32768).
---------------------------	---------------	---

## random-detect-group

To define the Weighted Random Early Detection (WRED) or distributed WRED (DWRED) parameter group, use the **random-detect group** global configuration command. To delete the WRED or DWRED parameter group, use the **no** form of this command.

**random-detect-group** *group-name* [*dscp-based* | *prec-based*]

**no random-detect-group** *group-name* [*dscp-based* | *prec-based*]

<b>Syntax Description</b>	<i>group-name</i>	Name for the WRED or DWRED parameter group.
	<i>dscp-based</i>	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
	<i>prec-based</i>	(Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.

## random-detect precedence

To configure Weighted Random Early Detection (WRED) and distributed WRED (DWRED) parameters for a particular IP Precedence, use the **random-detect precedence** interface configuration command. To configure WRED parameters for a particular IP Precedence for a class policy in a policy map, use the **random-detect precedence** policy-map class configuration command. To return the values to the default for the precedence, use the **no** form of this command.

**random-detect precedence** *precedence min-threshold max-threshold mark-prob-denominator*

**no random-detect precedence** *precedence min-threshold max-threshold mark-prob-denominator*

### Syntax Description

<i>precedence</i>	IP Precedence number. The value range is from 0 to 7. For Cisco 7000 series routers with an RSP7000 interface processor and Cisco 7500 series routers with a VIP2-40 interface processor (VIP2-50 interface processor strongly recommended), the precedence value range is from 0 to 7 only.
<i>min-threshold</i>	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP Precedence.
<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP Precedence.
<i>mark-prob-denominator</i>	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

## rate-limit

To configure committed access rate (CAR) and distributed CAR (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 conform-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 (bps). The value must be in increments of 8 kbps.
<i>burst-normal</i>	Normal burst size, in bytes. The minimum value is bps divided by 2000.
<i>burst-max</i>	Excess burst size, in bytes.
<b>conform-action</b> <i>conform-action</i>	<p>Action to take on packets that conform to 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 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>
--	--

## send qdm message

To send a text message to all Quality Device Manager (QDM) clients, use the **send qdm message EXEC** command.

```
send qdm [client client-id] message message-text
```

Syntax Description	
<b>client</b>	(Optional) Specifies a QDM client to receive the message.
<i>client-id</i>	(Optional) Specifies the QDM identification of the client that will receive the text message.
<b>message</b>	Specifies that a message will be sent.
<i>message-text</i>	The actual text of the message.

## service-policy

To attach a policy map to an input interface or virtual circuit (VC), or an output interface or VC, to be used as the service policy for that interface or VC, use the **service-policy** interface configuration command. To remove a service policy from an input or output interface or input or output VC, use the **no** form of this command.

**service-policy** {**input** | **output**} *policy-map-name*

**no service-policy** {**input** | **output**} *policy-map-name*

Syntax Description		
	<b>input</b>	Attaches the specified policy map to the input interface or input VC.
	<b>output</b>	Attaches the specified policy map to the output interface or output VC.
	<i>policy-map-name</i>	The name of a service policy map (created using the <b>policy-map</b> command) to be attached.

## service-policy (class-map)

To attach a policy map to a class, use the **service-policy** class-map configuration command. To remove a service policy from a class, use the **no** form of this command.

**service-policy** *policy-map*

**no service-policy**

Syntax Description		
	<i>policy-map</i>	The name of a service policy map (created using the <b>policy-map</b> command) to be attached.

## service-policy (policy-map class)

To use a service policy as a QoS policy within a policy map (called a hierarchical service policy), use the **service-policy** policy-map class configuration command. To disable a particular service policy as a QoS policy within a policy map, use the **no** form of this command.

**service-policy** *policy-map-name*

**no service-policy** *policy-map-name*

Syntax Description		
	<i>policy-map-name</i>	Specifies the name of the predefined policy map to be used as a QoS policy.

## set atm-clp

To control the cell loss priority (CLP) bit setting on Cisco routers when configuring a policy map, use the **set atm-clp** policy-map class configuration command.

```
set atm-clp
```

---

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

## set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **set cos** policy-map class configuration command. To remove a specific CoS value setting, use the **no** form of this command:

```
set cos cos-value
```

```
no set cos cos-value
```

---

<b>Syntax Description</b>	<i>cos-value</i>	Specific IEEE 802.1Q CoS value from 0 to 7.
---------------------------	------------------	---

---

## set ip dscp

To mark a packet by setting the IP differentiated services code point (DSCP) in the type of service (ToS) byte, use the **set ip dscp** policy-map configuration command. To remove a previously set IP DSCP, use the **no** form of this command.

```
set ip dscp ip-dscp-value
```

```
no set ip dscp ip-dscp-value
```

---

<b>Syntax Description</b>	<i>ip-dscp-value</i>	A number from 0 to 63 that sets the IP DSCP value. Reserved keywords <b>EF</b> (expedited forwarding), <b>AF11</b> (assured forwarding class AF11), and <b>AF12</b> (assured forwarding class AF12) can be specified instead of numeric values.
---------------------------	----------------------	---

---

## set ip precedence (policy-map)

To set the precedence value in the IP header, use the **set ip precedence** policy-map configuration command. To leave the precedence value at the current setting, use the **no** form of this command.

**set ip precedence** *ip-precedence-value*

**no set ip precedence**

---

<b>Syntax Description</b>	<i>ip-precedence-value</i>	A number from 0 to 7 that sets the precedence bit in the IP header.
---------------------------	----------------------------	---

---

## set ip precedence (route-map)

To set the precedence value (and an optional IP number or IP name) in the IP header, use the **set ip precedence** route-map configuration command. To leave the precedence value unchanged, use the **no** form of this command.

**set ip precedence** [*number* | *name*]

**no set ip precedence**

---

<b>Syntax Description</b>	<i>number</i>   <i>name</i>	(Optional) A number or name that sets the precedence bits in the IP header. The values for the <i>number</i> argument and the corresponding <i>name</i> argument are listed in Table 16, from least to most important.
---------------------------	-----------------------------	--

---

## set ip qos-group

To set a group ID that can be used later to classify packets, use the **set ip qos-group** route-map configuration command. To remove the group ID, use the **no** form of this command.

**set ip qos-group** *group-id*

**no set ip qos-group** *group-id*

---

<b>Syntax Description</b>	<i>group-id</i>	Group ID number in the range from 0 to 99.
---------------------------	-----------------	--

---

## set qos-group

To set a group ID that can be used later to classify packets, use the **set qos-group** policy-map configuration command. To remove the group ID, use the **no** form of this command.

```
set qos-group group-id
```

```
no set qos-group group-id
```

---

**Syntax Description**

---

<i>group-id</i>	Group ID number in the range from 0 to 99.
-----------------	--

---

■ set qos-group



## Quality of Service Commands: **shape** Through **vc-hold-queue**

---

This chapter describes the function and syntax of the quality of service (QoS) commands: **shape** through **vc-hold-queue**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Quality of Service Solutions Command Reference*.

### **shape**

To specify average or peak rate traffic shaping, use the **shape** class-map configuration command. To remove traffic shaping, use the **no** form of this command.

```
shape {average | peak} cir [bc] [be]
```

```
no shape {average | peak} cir [bc] [be]
```

---

#### **Syntax Description**

<b>average</b>	Specifies average rate shaping.
<b>peak</b>	Specifies peak rate shaping.
<i>cir</i>	Specifies the committed information rate (CIR), in bits per second (bps).
<i>bc</i>	(Optional) Specifies the Committed Burst rate, in bits.
<i>be</i>	(Optional) Specifies the Excess Burst rate, in bits.

---

### **shape (policy-map class)**

To shape traffic to the indicated bit rate according to the algorithm specified, use the **shape** policy-map class configuration command. To remove shaping and leaving the traffic unshaped, use the **no** form of this command.

```
shape [average | peak] mean-rate [[burst-size] [excess-burst-size]]
```

```
no shape [average | peak]
```

<b>Syntax Description</b>	<b>average</b>	(Optional) Committed Burst (Bc) is the maximum number of bits sent out in each interval.
	<b>peak</b>	(Optional) Bc + Excess Burst (Be) is the maximum number of bits sent out in each interval.
	<i>mean-rate</i>	(Optional) Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bits per second. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that will be permitted.
	<i>burst-size</i>	(Optional) The number of bits in a measurement interval (Bc).
	<i>excess-burst-size</i>	(Optional) The acceptable number of bits permitted to go over the Be.

## shape adaptive

To configure a Frame Relay interface or a point-to-point subinterface to estimate the available bandwidth by backward explicit congestion notification (BECN) integration while traffic shaping is enabled, use the **shape adaptive** policy-map class configuration command. If traffic shaping is not enabled, this command has no effect. To leave the available bandwidth unestimated, use the **no** form of this command.

**shape adaptive** *mean-rate-lower-bound*

**no shape adaptive**

<b>Syntax Description</b>	<i>mean-rate-lower-bound</i>	Specifies the lower bound of the range of permitted bit rates.
---------------------------	------------------------------	--

## shape fecn-adapt

To configure a Frame Relay interface to reflect received forward explicit congestion notification (FECN) bits as backward explicit congestion notification (BECN) bits in Q.922 TEST RESPONSE messages, use the **shape fecn-adapt** policy-map class configuration command. To configure the Frame Relay interface to not reflect FECN as BECN, use the **no** form of this command.

**shape fecn-adapt**

**no shape fecn-adapt**

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

## shape max-buffers

To specify the maximum number of buffers allowed on shaping queues, use the **shape max-buffers** class-map configuration command. To remove the maximum number of buffers, use the **no** form of this command.

```
shape max-buffers number-of-buffers
```

```
no shape max-buffers number-of-buffers
```

---

<b>Syntax Description</b>	<i>number-of-buffers</i>	Specifies the maximum number of buffers. The minimum number of buffers is 1; the maximum number of buffers is 4096.
---------------------------	--------------------------	---

---

## show access-lists rate-limit

To display information about rate-limit access lists, use the **show access-lists rate-limit EXEC** command.

```
show access-lists rate-limit [acl-index]
```

---

<b>Syntax Description</b>	<i>acl-index</i>	(Optional) Rate-limit access list number from 1 to 199.
---------------------------	------------------	---

---

## show atm bundle

To display the bundle attributes assigned to each bundle virtual circuit (VC) member and the current working status of the VC members, use the **show atm bundle** privileged EXEC command.

```
show atm bundle bundle-name
```

---

<b>Syntax Description</b>	<i>bundle-name</i>	The name of the bundle whose member information is displayed. This is the bundle name specified by the <b>bundle</b> command when the bundle was created.
---------------------------	--------------------	---

---

## show atm bundle statistics

To display statistics or detailed statistics on the specified bundle, use the **show atm bundle statistics** privileged EXEC command.

```
show atm bundle bundle-name statistics [detail]
```

<b>Syntax Description</b>	<i>bundle-name</i>	Specifies the name of the bundle whose member information is displayed. This is the bundle name specified by the <b>bundle</b> command when the bundle was created.
	<b>detail</b>	(Optional) Displays detailed statistics.

## show class-map

To display all class maps and their matching criteria, use the **show class-map** EXEC or privileged EXEC command.

```
show class-map [class-map-name]
```

<b>Syntax Description</b>	<i>class-map-name</i>	(Optional) Name of the class map.
---------------------------	-----------------------	-----------------------------------

## show cops servers

To display the IP address and connection status of the policy servers for which the router is configured, use the **show cops servers** EXEC command. The display also tells you about the Common Open Policy Service (COPS) client on the router.

```
show cops servers
```

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

## 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) Specifies interface number containing the data-link connection identifiers (DLCIs) for which you wish to display PVC information.
	<i>dlci</i>	(Optional) Specifies the DLCI number used on the interface. Statistics for the specified PVC are displayed when a DLCI is also specified.

## show interfaces fair-queue

To display information and statistics about weighted fair queueing (WFQ) for a Versatile Interface Processor (VIP)-based interface, use the **show interfaces fair-queue** EXEC command.

```
show interfaces [interface-type interface-number] fair-queue
```

---

### Syntax Description

<i>interface-type</i>	(Optional) The type of the interface.
-----------------------	---------------------------------------

<i>interface-number</i>	(Optional) The number of the interface.
-------------------------	---

---

## show interfaces random-detect

To display information about Weighted Random Early Detection (WRED) for a Versatile Interface Processor (VIP)-based interface, use the **show interfaces random-detect** EXEC command.

```
show interfaces [interface-type interface-number] random-detect
```

---

### Syntax Description

<i>interface-type</i>	(Optional) The type of the interface.
-----------------------	---------------------------------------

<i>interface-number</i>	(Optional) The number of the interface.
-------------------------	---

---

## show interfaces rate-limit

To display information about committed access rate (CAR) for an interface, use the **show interfaces rate-limit** EXEC command.

```
show interfaces [interface-type interface-number] rate-limit
```

---

### Syntax Description

<i>interface-type</i>	(Optional) The type of the interface.
-----------------------	---------------------------------------

<i>interface-number</i>	(Optional) The number of the interface.
-------------------------	---

---

## show ip nbar pdlm

To display the Packet Description Language Module (PDLM) in use by Network-Based Application Recognition (NBAR), use the **show ip nbar pdlm** privileged EXEC command.

```
show ip nbar pdlm
```

---

### Syntax Description

This command has no arguments or keywords.

## show ip nbar port-map

To display the current protocol-to-port mappings in use by Network-Based Application Recognition (NBAR), use the **show ip nbar port-map** privileged EXEC command.

```
show ip nbar port-map [protocol-name]
```

---

### Syntax Description

<i>protocol-name</i>	(Optional) Limits the command display to the specified protocol.
----------------------	--

---

## show ip nbar protocol-discovery

To display the statistics gathered by the Network-Based Application Recognition (NBAR) Protocol Discovery feature, use the **show ip nbar protocol-discovery** privileged EXEC command.

```
show ip nbar protocol-discovery [interface interface-spec] [stats {byte-count | bit-rate
| packet-count}][{protocol protocol-name | top-n number}]
```

---

### Syntax Description

<b>interface</b>	(Optional) Specifies that Protocol Discovery statistics for the interface are to be displayed.
<i>interface-spec</i>	(Optional) Specifies an interface to display.
<b>stats</b>	(Optional) Specifies that the byte count, byte rate, or packet count is to be displayed.
<b>byte-count</b>	(Optional) Specifies that the byte count is to be displayed.
<b>bit-rate</b>	(Optional) Specifies that the bit rate is to be displayed.
<b>packet-count</b>	(Optional) Specifies that the packet-count is to be displayed.
<b>protocol</b>	(Optional) Specifies that statistics for a specific protocol are to be displayed.
<i>protocol-name</i>	(Optional) User-specified protocol name for which the statistics are to be displayed.
<b>top-n</b>	(Optional) Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols will be displayed.
<i>number</i>	(Optional) Specifies the number of most active NBAR-supported protocols to be displayed.

---

## show ip rsvp

To display the IP Precedence bit values and type of service (ToS) bit values to be used to mark the ToS byte of the IP headers of all packets in a Resource Reservation Protocol (RSVP) reserved path that conform to or exceed the RSVP flowspec for a given interface, use the **show ip rsvp EXEC** command.

```
show ip rsvp {precedence | tos} [interface-name]
```

Syntax Description		
	<b>precedence</b>	Displays IP Precedence bit and ToS bit conform and exceed values for all interfaces on the router.  Either argument— <b>precedence</b> or <b>tos</b> —yields the same results. IP Precedence and ToS bit values for all interfaces with RSVP enabled are displayed in both cases.  Either <b>tos</b> or <b>precedence</b> may be specified; one is required.
	<b>tos</b>	Displays IP Precedence bit and ToS bit conform and exceed values for all interfaces on the router.  Either argument— <b>precedence</b> or <b>tos</b> —yields the same results. IP Precedence and ToS bit values for all interfaces with RSVP enabled are displayed in both cases.  Either <b>tos</b> or <b>precedence</b> may be specified; one is required.
	<i>interface-name</i>	(Optional) The name of the interface. If this argument is omitted, IP Precedence and ToS bit values are displayed for all interfaces with RSVP enabled.

## show ip rsvp atm-peak-rate-limit

To display the current peak rate limit set for an interface, if any, use the **show ip rsvp atm-peak-rate-limit EXEC** command.

```
show ip rsvp atm-peak-rate-limit [interface-name]
```

Syntax Description		
	<i>interface-name</i>	(Optional) The name of the interface.

## show ip rsvp installed

To display Resource Reservation Protocol (RSVP)-related installed filters and corresponding bandwidth information, use the **show ip rsvp installed EXEC** command.

```
show ip rsvp installed [detail][interface-type interface-number]
```

## ■ show ip rsvp interface

**Syntax Description**

<b>detail</b>	(Optional) Specifies additional information about interfaces and their reservations.
<i>interface-type</i>	(Optional) Specifies the type of the interface.
<i>interface-number</i>	(Optional) Specifies the number of the interface.

## show ip rsvp interface

To display Resource Reservation Protocol (RSVP)-related interface information, use the **show ip rsvp interface** EXEC command.

```
show ip rsvp interface [interface-type interface-number]
```

**Syntax Description**

<i>interface-type</i>	(Optional) Specifies the type of the interface.
<i>interface-number</i>	(Optional) Specifies the number of the interface.

## show ip rsvp neighbor

To display current Resource Reservation Protocol (RSVP) neighbors, use the **show ip rsvp neighbor** EXEC command.

```
show ip rsvp neighbor [interface-type interface-number]
```

**Syntax Description**

<i>interface-type</i>	(Optional) Specifies the type of the interface.
<i>interface-number</i>	(Optional) Specifies the number of the interface.

## show ip rsvp policy cops

To display the policy server addresses, access control list (ACL) IDs, and current state of the router-server connection, use the **show ip rsvp policy cops** command.

```
show ip rsvp policy cops [acl]
```

**Syntax Description**

[ <i>acl</i> ]	(Optional) The access control lists whose sessions are governed by Common Open Policy Service (COPS).
----------------	---

## show ip rsvp request

To display Resource Reservation Protocol (RSVP)-related request information being requested upstream, use the **show ip rsvp request** EXEC command.

**show ip rsvp request** [**detail**]

<b>Syntax Description</b>	<b>detail</b> (Optional) Specifies additional request information.
---------------------------	--

## show ip rsvp reservation

To display Resource Reservation Protocol (RSVP)-related receiver information currently in the database, use the **show ip rsvp reservation** EXEC command.

**show ip rsvp reservation** [**detail**]

<b>Syntax Description</b>	<b>detail</b> (Optional) Specifies additional reservation information.
---------------------------	--

## show ip rsvp sbm

To display information about a Subnetwork Bandwidth Manager (SBM) configured for a specific Resource Reservation Protocol (RSVP)-enabled interface or for all RSVP-enabled interfaces on the router, use the **show ip rsvp sbm** EXEC command.

**show ip rsvp sbm** [**detail**] [*interface-name*]

<b>Syntax Description</b>	<b>detail</b> (Optional) Detailed SBM configuration information, including values for the NonResvSendLimit object.
	<i>interface-name</i> (Optional) Name of the interface for which you want to display SBM configuration information.

## show ip rsvp sender

To display Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **show ip rsvp sender** EXEC command.

**show ip rsvp sender** [**detail**]

<b>Syntax Description</b>	<b>detail</b> (Optional) Specifies additional sender information.
---------------------------	---

## show policy-map

To display the configuration of all classes for a specified service policy map or all classes for all existing policy maps, use the **show policy-map** EXEC or privileged EXEC command.

```
show policy-map [policy-map]
```

---

### Syntax Description

<i>policy-map</i>	(Optional) The name of the service policy map whose complete configuration is to be displayed.
-------------------	--

---

## show policy-map class

To display the configuration for the specified class of the specified policy map, use the **show policy-map class** EXEC or privileged EXEC command.

```
show policy-map policy-map class class-name
```

---

### Syntax Description

<i>policy-map</i>	The name of a policy map that contains the class configuration to be displayed.
<i>class-name</i>	The name of the class whose configuration is to be displayed.

---

## show policy-map interface

To display the configuration of all classes configured for all service policies on the specified interface or to display the classes for the service policy for a specific permanent virtual circuit (PVC) on the interface, use the **show policy-map interface** EXEC or privileged EXEC command.

```
show policy-map interface interface-name [vc [vpi] vci][dlci dlci]
```

---

### Syntax Description

<i>interface-name</i>	Name of the interface or subinterface whose policy configuration is to be displayed.
<b>vc</b>	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC. The name can be up to 16 characters long.
<i>vpi</i>	(Optional) 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.  On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255.  The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.  If this value is omitted, information for all VCs on the specified ATM interface or subinterface is displayed.

---

<i>vci</i>	<p>(Optional) 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 (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signalling, Integrated Local Management Interface (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 <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p>
<b>dlci</b>	(Optional) Indicates a specific PVC for which policy configuration will be displayed.
<i>dlci</i>	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.

## show qdm status

To view the status of the Quality of Service Device Manager (QDM) clients connected to the router, use the **show qdm status EXEC** command.

```
show qdm status
```

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

## show queue

To display the contents of packets inside a queue for a particular interface or virtual circuit (VC), use the **show queue** privileged EXEC command.

```
show queue interface-name interface-number [vc [vpi/] vci]
```

<b>Syntax Description</b>	<i>interface-name</i>	The name of the interface.
	<i>interface-number</i>	The number of the interface.
	<b>vc</b>	(Optional) For ATM interfaces only, shows the fair queueing configuration for a specified permanent virtual circuit (PVC). The name can be up to 16 characters long.

<i>vpi</i>	<p>(Optional) 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.</p> <p>The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p> <p>If this value is omitted, information for all VCs on the specified ATM interface or subinterface is displayed.</p>
<i>vci</i>	<p>(Optional) 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-vp</b> command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signalling, Integrated Local Management Interface (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 <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.</p>

## show queueing

To list all or selected configured queueing strategies, use the **show queueing** privileged EXEC command.

```
show queueing [custom | fair | priority | random-detect [interface atm-subinterface
[vc [[vpi/] vci]]]]
```

Syntax Description	
<b>custom</b>	(Optional) Status of the custom queueing list configuration.
<b>fair</b>	(Optional) Status of the fair queueing configuration.
<b>priority</b>	(Optional) Status of the priority queueing list configuration.
<b>random-detect</b>	(Optional) Status of the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) configuration, including configuration of flow-based WRED.
<b>interface</b> <i>atm-subinterface</i>	(Optional) Displays the WRED parameters of every virtual circuit (VC) with WRED enabled on the specified ATM subinterface.
<b>vc</b>	(Optional) Displays the WRED parameters associated with a specific VC. If desired, both the virtual path identifier (VPI) and virtual circuit identifier (VCI) values, or just the VCI value, can be specified.
<i>vpi</i>	(Optional) Specifies the VPI. If the <i>vpi</i> argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the <i>vpi</i> argument is specified, the / separator is required.
<i>vci</i>	(Optional) Specifies the VCI.

## show queueing interface

To display the queueing statistics of an interface or a virtual circuit (VC), use the **show queueing interface** privileged EXEC command.

```
show queueing interface interface-number [vc [[vpi] vci]]
```

Syntax Description		
	<i>interface-number</i>	Specifies the number of the interface.
	<b>vc</b>	(Optional) Shows the weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) parameters associated with a specific VC. If desired, both the virtual path identifier (VPI) and virtual channel identifier (VCI) values, or just the VCI value, can be specified.
	<i>vpi</i>	(Optional) Specifies the VPI. If the <i>vpi</i> argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the <i>vpi</i> argument is specified, the / separator is required.
	<i>vci</i>	(Optional) Specifies the VCI.

## show tech-support rsvp

To generate a report of all Resource Reservation Protocol (RSVP)-related information, use the **show tech-support rsvp** privileged EXEC command.

```
show tech-support rsvp
```

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

## show traffic-shape

To display the current traffic-shaping configuration, use the **show traffic-shape** EXEC command.

```
show traffic-shape [interface-type interface-number]
```

Syntax Description		
	<i>interface-type</i>	(Optional) The type of the interface. If no interface is specified, traffic-shaping details for all configured interfaces are shown.
	<i>interface-number</i>	(Optional) The number of the interface.

## show traffic-shape queue

To display information about the elements queued by traffic shaping at the interface level or the data-link connection identifier (DLCI) level, use the **show traffic-shape queue** EXEC command.

```
show traffic-shape queue [interface-number [dcli dcli-number]]
```

<b>Syntax Description</b>	<i>interface-number</i>	(Optional) The number of the interface.
	<b>dlci</b>	(Optional) The specific DLCI for which you wish to display information about queued elements.
	<i>dlci-number</i>	(Optional) The number of the DLCI.

## show traffic-shape statistics

To display the current traffic-shaping statistics, use the **show traffic-shape statistics EXEC** command.

```
show traffic-shape statistics [interface-type interface-number]
```

<b>Syntax Description</b>	<i>interface-type</i>	(Optional) The type of the interface. If no interface is specified, traffic-shaping statistics for all configured interfaces are shown.
	<i>interface-number</i>	(Optional) The number of the interface.

## traffic-shape adaptive

To configure a Frame Relay subinterface to estimate the available bandwidth when backward explicit congestion notification (BECN) signals are received, use the **traffic-shape adaptive** interface configuration command. To disregard the BECN signals and not estimate the available bandwidth, use the **no** form of this command.

```
traffic-shape adaptive bit-rate
```

```
no traffic-shape adaptive
```

<b>Syntax Description</b>	<i>bit-rate</i>	Lowest bit rate that traffic is shaped to, in bits per second. The default <i>bit rate</i> value is 0.
---------------------------	-----------------	--

## traffic-shape fecn-adapt

To reply to messages with the forward explicit congestion notification (FECN) bit (which are sent with TEST RESPONSE messages with the BECN bit set), use the **traffic-shape fecn-adapt** interface configuration command. To stop backward explicit congestion notification (BECN) signal generation, use the **no** form of this command.

```
traffic-shape fecn-adapt
```

```
no traffic-shape fecn-adapt
```

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

## traffic-shape group

To enable traffic shaping based on a specific access list for outbound traffic on an interface, use the **traffic-shape group** interface configuration command. To disable traffic shaping on the interface for the access list, use the **no** form of this command.

**traffic-shape group** *access-list* *bit-rate* [*burst-size* [*excess-burst-size*]]

**no traffic-shape group** *access-list*

Syntax Description		
	<i>access-list</i>	Number of the access list that controls the packets that traffic shaping is applied to on the interface.
	<i>bit-rate</i>	Bit rate that traffic is shaped to, in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain.
	<i>burst-size</i>	(Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the Committed Burst size contracted with your service provider.
	<i>excess-burst-size</i>	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the Excess Burst size contracted with your service provider. The default is equal to the <i>burst-size</i> argument.

## traffic-shape rate

To enable traffic shaping for outbound traffic on an interface, use the **traffic-shape rate** interface configuration command. To disable traffic shaping on the interface, use the **no** form of this command.

**traffic-shape rate** *bit-rate* [*burst-size* [*excess-burst-size*]]

**no traffic-shape rate**

Syntax Description		
	<i>bit-rate</i>	Bit rate that traffic is shaped to, in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain.
	<i>burst-size</i>	(Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the Committed Burst size contracted with your service provider.
	<i>excess-burst-size</i>	(Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the Excess Burst size contracted with your service provider. The default is equal to the <i>burst-size</i> argument.

## tx-ring-limit

To limit the number of particles that can be used on a transmission ring on the PA-A3 port adapter, use the **tx-ring-limit** ATM VC configuration command. To not limit the number of particles that can be used on a transmission ring on a PA-A3 port adapter, use the **no** form of this command.

**tx-ring-limit** *ring-limit*

**no tx-ring-limit** *ring-limit*

<b>Syntax Description</b>	<i>ring-limit</i>	Specifies the maximum number of allowable particles that can be placed on the transmission ring.
---------------------------	-------------------	--

## vc-hold-queue

To configure the per-virtual circuit (VC) hold queue on an ATM adapter, use the **vc-hold-queue** interface configuration command. To return to the default value of the per-VC hold queue, use the **no** form of this command.

**vc-hold-queue** *number-of-packets*

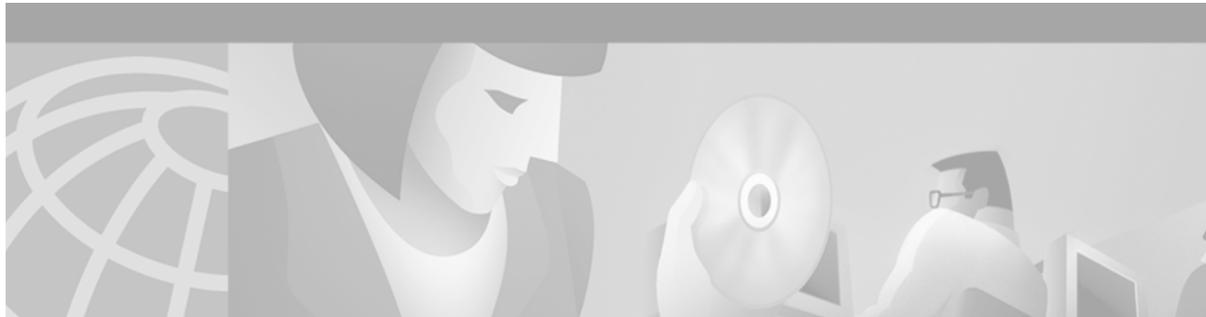
**no vc-hold-queue** *number-of-packets*

<b>Syntax Description</b>	<i>number-of-packets</i>	Specifies number of packets that can be configured for the per-VC hold queue. Number of packets can be a minimum of 5 to a maximum of 1024.
---------------------------	--------------------------	---



**Voice, Video, and Fax**





## Voice, Video, and Fax Commands: **acc-qos** Through **customer-id**

---

This chapter describes the function and syntax of the voice, video, and fax commands from **acc-qos** through **customer-id**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Voice, Video, and Fax Command Reference*.

### **acc-qos**

To define the acceptable quality of service (QoS) for any inbound and outbound call on a Voice over IP (VoIP) dial peer, use the **acc-qos** command in dial peer configuration mode. To restore the default QoS setting, use the **no** form of this command.

```
acc-qos {best-effort | controlled-load | guaranteed-delay}
```

```
no acc-qos
```

<b>Syntax Description</b>		
	<b>best-effort</b>	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation. This is the default.
	<b>controlled-load</b>	Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.
	<b>guaranteed-delay</b>	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

### **alarm-trigger**

To configure a T1 or E1 controller to send an alarm to the public switched telephone network (PSTN) or switch if specified T1 or E1 DS0 groups are out of service, use the **alarm-trigger** command in controller configuration mode. To configure a T1 or E1 controller not to send an alarm, use the **no** form of this command.

```
alarm-trigger blue ds0-group-list
```

```
no alarm-trigger
```

<b>Syntax Description</b>	<b>blue</b>	Specifies the alarm type to be sent is “blue,” also know as an Alarm Indication Signal (AIS).
	<i>ds0-group-list</i>	Specifies the DS0 group or groups to be monitored for permanent trunk connection status or busyout status.

## alias static

To create a static entry in the local alias table, use the **alias static** command in gatekeeper configuration mode. To remove a static entry, use the **no** form of this command.

```
alias static ip-signaling-addr [port] gkid gatekeeper-name [ras ip-ras-addr port] [terminal | mcu | gateway {h320 | h323-proxy | voip}] [e164 e164-address] [h323id h323-id]
```

```
no alias static ip-signaling-addr [port] gkid gatekeeper-name [ras ip-ras-addr port] [terminal | mcu | gateway {h320 | h323-proxy | voip}] [e164 e164-address] [h323id h323-id]
```

<b>Syntax Description</b>	<i>ip-signaling-addr</i>	IP address of the H.323 node, used as the address to signal when establishing a call.
	<i>port</i>	(Optional) Port number other than the endpoint Call Signaling well-known port number (1720).
	<b>gkid</b> <i>gatekeeper-name</i>	Name of the local gatekeeper of whose zone this node is a member.
	<b>ras</b> <i>ip-ras-addr</i>	(Optional) Node remote access server (RAS) signaling address. If omitted, the <i>ip-signaling-addr</i> parameter is used in conjunction with the RAS well-known port.
	<i>port</i>	(Optional) Port number other than the RAS well-known port number (1719).
	<b>terminal</b>	(Optional) Indicates that the alias refers to a terminal.
	<b>mcu</b>	(Optional) Indicates that the alias refers to a multiple control unit (MCU).
	<b>gateway</b>	(Optional) Indicates that the alias refers to a gateway.
	<b>h320</b>	(Optional) Indicates that the alias refers to an H.320 node.
	<b>h323-proxy</b>	(Optional) Indicates that the alias refers to an H.323 proxy.
	<b>voip</b>	(Optional) Indicates that the alias refers to VoIP.
	<b>e164</b> <i>e164-address</i>	(Optional) Specifies the node E.164 address. This keyword and argument can be used more than once to specify as many E.164 addresses as needed. Note that there is a maximum number of 128 characters that can be entered for this address. To avoid exceeding this limit, you can enter multiple <b>alias static</b> commands with the same call signaling address and different aliases.
	<b>h323id</b> <i>h323-id</i>	(Optional) Specifies the node H.323 alias. This keyword and argument can be used more than once to specify as many H.323 identification (ID) aliases as needed. Note that there is a maximum number of 256 characters that can be entered for this address. To avoid exceeding this limit, you can enter multiple <b>alias static</b> commands with the same call signaling address and different aliases.

## alt-dial

To configure an alternate dial-out string for dial peers on the Cisco MC3810, use the **alt-dial** command in dial peer configuration mode. To delete the alternate dial-out string, use the **no** form of this command.

**alt-dial** *string*

**no alt-dial** *string*

Syntax Description	
<i>string</i>	The alternate dial-out string.

## answer-address

To specify the full E.164 telephone number to be used to identify the dial peer of an incoming call, use the **answer-address** command in dial peer configuration mode. To disable the configured telephone number, use the **no** form of this command.

**answer-address** [**+**]*string*[**T**]

**no answer-address**

Syntax Description	
<b>+</b>	(Optional) Character indicating an E.164 standard number.
<i>string</i>	Series of digits that specify the E.164 or private dial plan telephone number. Valid entries are as follows: <ul style="list-style-type: none"> <li>• Digits 0 through 9, letters A through D, pound sign (#), and asterisk (*), which represent specific digits that can be entered.</li> <li>• Comma (,), which inserts a pause between digits.</li> <li>• Period (.), which matches any entered digit.</li> </ul>
<b>T</b>	(Optional) Control character indicating that the <b>answer-address</b> value is a variable-length dial string.



## application

To enable a specific application on a dial peer, use the **application** command in dial peer configuration mode. To remove the application from the dial peer, use the **no** form of this command.

**application** *application-name* [**out-bound**]

**no application** *application-name* [**out-bound**]

<b>Syntax Description</b>	<i>application-name</i>	Indicates the name of the predefined application you wish to enable on the dial peer. For H.323 networks, the application is defined by a Tool Command Language/interactive voice response (TCL/IVR) filename and location. Incoming calls using plain old telephone service (POTS) dial peers and outgoing calls using Multimedia Mail over IP (MMOIP) dial peers are handed off to this application.
---------------------------	-------------------------	--

## arq reject-unknown-prefix

To enable the gatekeeper to reject admission requests (ARQs) for zone prefixes that are not configured, use the **arq reject-unknown-prefix** command in gatekeeper configuration mode. To reenable the gatekeeper to accept and process all incoming ARQs, use the **no** form of this command.

**arq reject-unknown-prefix**

**no arq reject-unknown-prefix**

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

## atm compression

To specify the software compression mode on an interface, use the **atm compression** command in interface configuration mode. To remove the compression mode setting, use the **no** form of this command.

**atm compression {per-packet | per-interface | per-vc}**

**no atm compression {per-packet | per-interface | per-vc}**

<b>Syntax Description</b>	<b>per-packet</b>	Specifies packet-by-packet compression mode (no history). This is the default.
	<b>per-interface</b>	Specifies one context per interface (with history).
	<b>per-vc</b>	Specifies one context for every virtual circuit (with history).

## atm scramble-enable

To enable scrambling on E1 links, use the **atm scramble-enable** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

**atm scramble-enable**

**no atm scramble-enable**

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

## atm video aesa

To set the unique ATM end-station address (AESA) for an ATM video interface that is using switched virtual circuit (SVC) mode, use the **atm video aesa** command in ATM interface configuration mode. To remove any configured address for the interface, use the **no** form of this command.

```
atm video aesa [default | esi-address]
```

```
no atm video aesa
```

Syntax Description	default	(Optional) Automatically creates a network service access point (NSAP) address for the interface, based on a prefix from the ATM switch (26 hexadecimal characters), the MAC address (12 hexadecimal characters) as the end station identifier (ESI), and a selector byte (two hexadecimal characters).
	<i>esi-address</i>	(Optional) Defines the 12 hexadecimal characters used as the ESI. The ATM switch provides the prefix (26 hexadecimal characters), and the video selector byte provides the remaining two hexadecimal characters.

## audio-prompt load

To initiate loading the selected audio file (.au), the file that contains the announcement prompt for the caller from Flash memory into RAM, use the **audio-prompt load** command in privileged EXEC mode.

```
audio-prompt load name
```

Syntax Description	<i>name</i>	Indicates the location of the audio file that you want to have loaded from memory, Flash memory, or an FTP server.
--------------------	-------------	--

## auto-cut-through

To enable call completion when a PBX does not provide an M-lead response, use the **auto-cut-through** command in voice-port configuration mode. To disable the auto-cut-through operation, use the **no** form of this command.

```
auto-cut-through
```

```
no auto-cut-through
```

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

## bandwidth

To specify the maximum aggregate bandwidth for H.323 traffic, use the **bandwidth** command in gatekeeper configuration mode. To remove the maximum aggregate bandwidth value, use the **no** form of this command.

**bandwidth** {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*} *bandwidth-size*

**no bandwidth** {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*} *bandwidth-size*

Syntax Description		
<b>interzone</b>		Specifies the maximum bandwidth for H.323 traffic between one zone and another zone.
<b>total</b>		Specifies the maximum bandwidth for H.323 traffic within a zone and between zones (intrazone and interzone).
<b>session</b>		Specifies the maximum bandwidth allowed for a single session in a specific zone or in all zones.
<b>default</b>		Specifies the maximum bandwidth for all applicable zones, depending on the keyword with which it is used.
<b>zone</b>		Specifies a particular zone.
<i>zone-name</i>		Names the particular zone.
<i>bandwidth-size</i>		Maximum bandwidth. For <b>interzone</b> and <b>total</b> , the range is from 1 to 10,000,000 kbps. For <b>session</b> , the range is from 1 to 5000 kbps.

## bandwidth remote

To specify the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper, use the **bandwidth remote** command in gatekeeper configuration mode. To disable, use the **no** form of this command.

**bandwidth remote** *bandwidth-size*

**no bandwidth remote** *bandwidth-size*

Syntax Description		
<i>bandwidth-size</i>		Maximum bandwidth. The range is from 1 to 10,000,000 kbps.

## battery-reversal

To specify battery polarity reversal on a Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) port, use the **battery-reversal** command in voice-port configuration mode. To disable battery reversal, use the **no** form of this command.

**battery-reversal**

**no battery-reversal**

Syntax Description	
	This command has no arguments or keywords.

## block-caller

To configure call blocking on caller ID, use the **block-caller** command in dial peer voice configuration mode. To disable call blocking on caller ID, use the **no** form of this command.

**block-caller** *number*

**no block-caller** *number*

<b>Syntax Description</b>	number	Specifies the telephone number to block. You can use a period (.) as a digit wildcard. For example, the command <b>block-caller 5.51234</b> blocks all numbers beginning with the digit 5, followed by any digit, and then sequentially followed by the digits 5, 1, 2, 3, and 4.
---------------------------	--------	---

## busyout forced

To force a voice port into the busyout state, use the **busyout forced** command in voice-port configuration mode. To remove the voice port from the busyout state, use the **no** form of this command.

**busyout forced**

**no busyout forced**

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

## busyout monitor

To place a voice port into the busyout monitor state, enter the **busyout monitor** command in voice-port configuration mode. To remove the busyout monitor state from the voice port, use the **no** form of this command.

**busyout monitor** {*serial interface-number* | *ethernet interface-number*} [**in-service**]

**no busyout monitor** {*serial interface-number* | *ethernet interface-number*}

<b>Syntax Description</b>	<b>serial</b>	Specifies monitoring of a serial interface.
		 <b>Note</b> More than one interface can be entered for a voice port.
		 <b>Note</b> The Cisco 2600 and 3600 series routers and the MC3810 multiservice concentrator support ATM interfaces. To monitor an ATM interface, enter <b>ATM</b> and the interface number.
	<b>ethernet</b>	Specifies monitoring of an Ethernet interface.
		 <b>Note</b> More than one interface can be entered for a voice port.
	<i>interface-number</i>	Identifies an interface to be monitored for the voice port busyout function. Interface choices include serial port, serial port subinterface, Ethernet port, and ATM interface.
	<b>in-service</b>	(Optional) Configures the voice port to be busied out when any monitored interface comes into service (its state changes to up). If the keyword is not entered, the voice port is busied out when all monitored interfaces go out of service (their state changes to down).

## busyout monitor probe

To configure a voice port to enter the busyout state if a response time reporter (RTR) probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold, use the **busyout monitor probe** command in voice-port configuration mode. To configure a voice port not to monitor RTR probe signals, use the **no** form of this command.

**busyout monitor probe** *ip-address* [**codec** *codec-type*] [**icpif** *number* | **loss percent delay** *milliseconds*]

**no busyout monitor probe** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i>	The IP address of a target interface for the RTR probe signal.
	<b>codec</b>	(Optional) Configures the profile of the RTR probe signal to mimic the packet size and interval of a specific codec type.

<i>codec-type</i>	(Optional) The codec type for the RTR probe signal. Available options are as follows: <ul style="list-style-type: none"> <li>• g711a—G.711 A-law</li> <li>• g711u—G.711 U-law (the default)</li> <li>• g729—G.729</li> <li>• g729a—G.729</li> </ul>
<b>icpif</b>	(Optional) Configures the busyout monitor probe to use an Impairment/Calculated Planning Impairment Factor (ICPIF) loss/delay busyout threshold, in accordance with ITU-T G.113. The ICPIF numbers represent predefined combinations of loss and delay.
<i>number</i>	(Optional) The ICPIF threshold for initiating a busyout. The range is from 0 to 30. Lower numbers are equivalent to lower loss and delay thresholds.
<b>loss</b>	(Optional) Configures the percentage-of-packets-lost threshold for initiating a busyout.
<i>percent</i>	(Optional) The loss value (expressed as a percentage) for initiating a busyout. The range is from 1 to 100.
<b>delay</b>	(Optional) Configures the average packet delay threshold for initiating a busyout.
<i>milliseconds</i>	(Optional) The delay threshold, in milliseconds, for initiating a busyout. The range is from 1 to 2147483647.

## busyout seize

To change the busyout action for an Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) voice port, use the **busyout seize** command in voice-port configuration mode. To restore the default busyout action, use the **no** form of this command.

**busyout seize** {**ignore** | **repeat**}

**no busyout seize**

Syntax Description	
<b>ignore</b>	Specifies the type of ignore procedure, depending on the type of voice port signaling.
<b>repeat</b>	Specifies the type of repeat procedure, depending on the type of voice port signaling.

## cac master

To configure the call admission control (CAC) operation as master, enter the **cac master** command in voice-service configuration mode. To restore the default value, use the **no** form of this command.

**cac master**

**no cac master**

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

## cadence-list

To specify a tone cadence pattern to be detected, use the **cadence-list** command in voice-class configuration mode. To delete a cadence pattern, use the **no** form of this command.

**cadence-list** *cadence-id* *cycle-1-on-time* *cycle-1-off-time* [*cycle-2-on-time* *cycle-2-off-time*]  
[*cycle-3-on-time* *cycle-3-off-time*] [*cycle-4-on-time* *cycle-4-off-time*]

**no cadence-list** *cadence-id*

Syntax Description	
<i>cadence-id</i>	A tag to identify this cadence list. The range is from 1 to 10.
<i>cycle-1-on-time</i>	The tone duration for the first cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
<i>cycle-1-off-time</i>	The silence duration for the first cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
<i>cycle-2-on-time</i>	(Optional) The tone duration for the second cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
<i>cycle-2-off-time</i>	(Optional) The silence duration for the second cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
<i>cycle-3-on-time</i>	(Optional) The tone duration for the third cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
<i>cycle-3-off-time</i>	(Optional) The silence duration for the third cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
<i>cycle-4-on-time</i>	(Optional) The tone duration for the fourth cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.
<i>cycle-4-off-time</i>	(Optional) The silence duration for the fourth cycle of the cadence pattern. The range is from 0 to 1000 (0 milliseconds to 100 seconds). The default is 0.

## cadence-max-off-time

To specify the maximum off duration for detection of a tone, use the **cadence-max-off-time** command in voice-class configuration mode. To restore the default, use the **no** form of this command.

**cadence-max-off-time** *time*

**no cadence-max-off-time**

<b>Syntax Description</b>	<i>time</i>	The maximum off time of the tone that can be detected, in 10-millisecond increments. The range is from 0 to 5000 (0 milliseconds to 50 seconds). The default is 0.
---------------------------	-------------	--

## cadence-min-on-time

To specify the minimum on duration for detection of a tone, use the **cadence-min-on-time** command in voice-class configuration mode. To restore the default, use the **no** form of this command.

**cadence-min-on-time** *time*

**no cadence-min-on-time**

<b>Syntax Description</b>	<i>time</i>	The minimum on time of a tone that can be detected, in 10-millisecond increments. The range is from 0 to 100 (0 milliseconds to 1 seconds). The default is 0.
---------------------------	-------------	---

## cadence-variation

To specify the cadence variation time allowed for detection of a tone, use the **cadence-variation** command in voice-class configuration mode. To restore the default cadence variation time, use the **no** form of this command.

**cadence-variation** *time*

**no cadence-variation**

<b>Syntax Description</b>	<i>time</i>	The maximum time by which the tone onset can vary from the specified onset time and still be detected, in 10-millisecond increments. The range is from 0 to 200 (0 milliseconds to 2 seconds). The default is 0.
---------------------------	-------------	--

## call application cache reload time

To configure the router to reload the Media Gateway Control Protocol (MGCP) scripts from cache on a regular interval, use the **call application cache reload time** command in global configuration mode. To set the value to the default, use the **no** form of this command.

**call application cache reload time** *bg-minutes*

**no call application cache reload time**

<b>Syntax Description</b>	<i>bg-minutes</i>	<p>Specifies the number of minutes after which the background process is awakened. This background process checks the time elapsed since the script was last used and whether the script is current:</p> <ul style="list-style-type: none"> <li>• If the script has not been used in the last “unload time,” it will unload the script and quit. The unload time is not configurable.</li> <li>• If the script has been used, the background process will load the script from the URL. It compares the scripts, and if they do not match, it begins using the new script for new calls.</li> </ul>
---------------------------	-------------------	---

## call application voice

To create an application and to indicate the location of the corresponding Tool Command Language (TCL) files that implement this application, use the **call application voice** command in global configuration mode. To remove the defined application and all configured parameters associated with it, use the **no** form of this command.

**call application voice** *application-name location {word}*

**no call application voice** *application-name location {word}*

<b>Syntax Description</b>	<i>application-name</i>	Character string that defines the name of the application.
	<i>location</i>	Location of the TCL file in URL format. Valid storage locations are TFTP, FTP, and Flash.
	<i>word</i>	Text string that defines an attribute-value pair specified by the TCL script and understood by the RADIUS server.

## call application voice access-method

To specify the access method for two-stage dialing for the designated application, use the **call application voice access-method** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

**call application voice** *application-name access-method {prompt-user | redialer}*

**no call application voice** *application-name access-method*

<b>Syntax Description</b>	<i>application-name</i>	The name of the application.
	<b>prompt-user</b>	Specifies that no direct inward dialing (DID) is set in the incoming plain old telephone service (POTS) dial peer and that a Tool Command Language (TCL) script in the incoming POTS dial peer will be used for two-stage dialing.
	<b>redialer</b>	Specifies that no DID is set in the incoming POTS dial peer and that the redialer device will be used for two-stage dialing.

## call application voice accounting enable

To enable authentication, authorization, and accounting (AAA) accounting for a Tool Command Language (TCL) application, use the **call application voice accounting enable** command in global configuration mode. To disable accounting for a TCL application, use the **no** form of this command.

**call application voice** *application-name* **accounting enable**

**no call application voice** *application-name* **accounting enable**

<b>Syntax Description</b>	<i>application-name</i>	The name of the application.
---------------------------	-------------------------	------------------------------

## call application voice accounting-list

To define the accounting list name of the voice feature card (VFC), use the **call application voice accounting-list** command in global configuration mode. To restore the default value, use the **no** form of this command.

**call application voice** *application-name* **accounting-list** *method-list-name*

**no call application voice** *application-name* **accounting-list** *method-list-name*

<b>Syntax Description</b>	<i>application-name</i>	The name of the application.
	<i>method-list-name</i>	Character string used to name a list of accounting methods to be used with store-and-forward fax.

## call application voice authen-list

To specify the name of an authentication method list for a Tool Command Language (TCL) application, use the **call application voice authen-list** command in global configuration mode. To disable the authentication method list for a TCL application, use the **no** form of this command.

**call application voice** *application-name* **authen-list** *method-list-name*

**no call application voice** *application-name* **authen-list** *method-list-name*

<b>Syntax Description</b>	<i>application-name</i>	The name of the application.
	<i>method-list-name</i>	Character string used to name a list of authentication methods to be used with T.38 fax relay and T.37 store-and-forward fax.

## call application voice authen-method

To specify an authentication, authorization, and accounting (AAA) authentication method for a Tool Command Language (TCL) application, use the **call application voice authen-method** command in global configuration mode. To disable the authentication method for a TCL application, use the **no** form of this command.

```
call application voice application-name authen-method {prompt-user | ani | dnis | gateway | redialer-id | redialer-dnis}
```

```
no call application voice application-name authen-method {prompt-user | ani | dnis | gateway | redialer-id | redialer-dnis}
```

<b>Syntax Description</b>	<i>application-name</i>	The name of the application.
	<b>prompt-user</b>	Indicates that the user is prompted for the TCL application account identifier.
	<b>ani</b>	Indicates that the calling-party telephone number (automatic number identification [ANI]) is used as the TCL application account identifier.
	<b>dnis</b>	Indicates that the called party telephone number (dialed number identification service [DNIS]) is used as the TCL application account identifier.
	<b>gateway</b>	Indicates that the router-specific name derived from the host name and domain name is used as the TCL application account identifier. It is displayed in the following format: <i>router-name.domain-name</i> .
	<b>redialer-id</b>	Indicates that the account string returned by the external redialer device is used as the TCL application account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
	<b>redialer-dnis</b>	Indicates that the called party telephone number (dialed number identification service or DNIS) is used as the TCL application account identifier captured by the redialer if a redialer device is present.

## call application voice global-password

To define a password to be used with CiscoSecure for Windows NT when using store-and-forward fax on a voice feature card, use the **call application voice global-password** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
call application voice application-name global-password password
```

```
no call application voice application-name global-password password
```

<b>Syntax Description</b>	<i>application-name</i>	The name of the application.
	<i>password</i>	Character string used to define the CiscoSecure for Windows NT password to be used with store-and-forward fax. The maximum length is 64 alphanumeric characters.

## call application voice language

To define the language of the audio file for the specified application and to pass that information to the specified application, use the **call application voice language** command in global configuration mode. To remove the associated language of the audio file from the application, use the **no** form of this command.

**call application voice** *application-name* **language** *number* *language*

**no call application voice** *application-name* **language** *number* *language*

<b>Syntax Description</b>	<i>application-name</i>	The name of the application to which the language parameters are being passed.
	<i>number</i>	Tag that uniquely identifies an audio file. Valid entries are from 0 to 9.
	<i>language</i>	Defines the language of the associated audio file. Valid entries are as follows: <ul style="list-style-type: none"> <li>• <b>en</b>—English</li> <li>• <b>sp</b>—Spanish</li> <li>• <b>ch</b>—Mandarin</li> <li>• <b>aa</b>—all</li> </ul>

## call application voice load

To reload the selected Tool Command Language (TCL) script from the URL, use the **call application voice load** command in privileged EXEC mode.

**call application voice load** *name*

<b>Syntax Description</b>	<i>name</i>	Defines the TCL script to use for the call. Enter the name of the TCL or Media Gateway Control Protocol (MGCP) script you want this dial peer to use.
---------------------------	-------------	---

## call application voice pin-len

To define the number of characters in the personal identification number (PIN) for the designated application, use the **call application voice pin-len** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

**call application voice** *application-name* **pin-len** *number*

**no call application voice** *application-name* **pin-len** *number*

### Syntax Description

<i>application-name</i>	The name of the application to which the PIN length parameter is being passed.
<i>number</i>	Defines the number of allowable characters in PINs associated with the specified application. Valid entries are from 0 to 10.

## call application voice redirect-number

To define the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application, use the **call application voice redirect-number** command in global configuration mode. To cancel this particular parameter, use the **no** form of this command.

**call application voice** *application-name* **redirect-number** *number*

**no call application voice** *application-name* **redirect-number** *number*

### Syntax Description

<i>application-name</i>	The name of the application to which the redirect telephone number parameter is being passed.
<i>number</i>	Defines the designated operator telephone number of the service provider (or any other number designated by the customer). This is the number that calls are terminated to when, for example, debit time allowed has run out or the debit amount is exceeded.

## call application voice retry-count

To define the number of times a caller is permitted to reenter the personal identification number (PIN) for the designated application, use the **call application voice retry-count** command in global configuration mode. To cancel this particular parameter, use the **no** form of this command.

**call application voice** *application-name* **retry-count** *number*

**no call application voice** *application-name* **retry-count** *number*

Syntax Description		
	<i>application-name</i>	The name of the application to which the number of possible retries is being passed.
	<i>number</i>	Defines the number of times the caller is permitted to reenter personal identification number (PIN) digits. Valid entries for this parameter are from 1 to 5.

## call application voice set-location

To define the location, language, and category of the audio files for the specified application, use the **call application voice set-location** command in global configuration mode. To cancel this particular parameter, use the **no** form of this command.

**call application voice** *application-name* **set-location** *language category location*

**no call application voice** *application-name* **set-location** *language category location*

Syntax Description		
	<i>application-name</i>	The name of the application to which the <b>set-location</b> parameters are being passed.
	<i>language</i>	Defines the language associated with the audio files. Possible values for this parameter are as follows: <ul style="list-style-type: none"> <li><b>en</b> = English</li> <li><b>ch</b> = Mandarin</li> <li><b>sp</b> = Spanish</li> </ul>
	<i>category</i>	Defines a particular category group. Audio files can be divided into category groups (from 0 to 4). For example, audio files representing the days and months can be category 1, audio files representing units of currency can be category 2, audio files representing units of time—seconds, minutes, and hours—can be category 3. The minimum is 0; the maximum is 4 (0 means all).
	<i>location</i>	Defines the location (audio file URL or directory in the TFTP server) where the audio files are stored.

## call application voice uid-length

To define the number of characters in the user identification number (UID) for the designated application, use the **call application voice uid-length** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

**call application voice** *application-name* **uid-len** *number*

**no call application voice** *application-name* **uid-len** *number*

Syntax Description		
	<i>application-name</i>	The name of the application to which the UID length parameter is being passed.
	<i>number</i>	Defines the number of allowable characters in UIDs associated with the specified application. Valid entries are from 1 to 20.

## call application voice warning-time

To define the number of second's warning that a user receives before the allowed calling time runs out, use the **call application voice warning-time** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

**call application voice** *application-name* **warning-time** *number*

**no call application voice** *application-name* **warning-time** *number*

### Syntax Description

<i>application-name</i>	The name of the application to which the warning time parameter is being passed.
<i>number</i>	Defines the length of the warning period, in seconds, before the allowed calling time runs out. Valid entries are from 10 to 600.

## call fallback active

To enable a call request to fall back to alternate dial peers in case of network congestion, use the **call fallback active** command in global configuration mode. To disable public switched telephone network (PSTN) fall back, use the **no** form of this command.

**call fallback active**

**no call fallback active**

### Syntax Description

This command has no arguments or keywords.

## call fallback cache-size

To specify the call fall back cache size for network traffic probe entries, use the **call fallback cache-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

**call fallback cache-size** *number*

**no call fallback cache-size** *number*

### Syntax Description

<i>number</i>	Specifies the cache size in number of entries. The valid range is from 1 to 256.
---------------	--

## call fallback cache-timeout

To specify the time after which the cache entries of network conditions are purged, use the **call fallback cache-timeout** command in global configuration mode. To disable, use the **no** form of this command.

**call fallback cache-timeout** *seconds*

**no call fallback cache-timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Specifies the cache timeout value in seconds. The valid range is from 1 to 2,147,483.
---------------------------	----------------	---

## call fallback instantaneous-value-weight

To configure the call fallback subsystem to take an average from the last two probes registered in the cache for call requests, use the **call fallback instantaneous-value-weight** command in global configuration mode. To return to the default values, use the **no** form of this command.

**call fallback instantaneous-value-weight** *weight*

**no call fallback instantaneous-value-weight** *weight*

<b>Syntax Description</b>	<i>weight</i>	Specifies the instantaneous value weight. The valid range is from 0 to 100 percent.
---------------------------	---------------	---

## call fallback jitter-probe num-packets

To specify the number of packets in a jitter probe used to determine network conditions, use the **call fallback jitter-probe num-packets** command in global configuration mode. To restore the default value, use the **no** form of this command.

**call fallback jitter-probe num-packets** *number-of-packets*

**no call fallback jitter-probe num-packets** *number-of-packets*

<b>Syntax Description</b>	<i>number-of-packets</i>	Specifies the number of packets value. The valid range is from 2 to 50.
---------------------------	--------------------------	---

## call fallback jitter-probe precedence

To specify the treatment of the jitter-probe transmission, use the **call fallback jitter-probe precedence** command in global configuration mode. To restore the default value, use the **no** form of this command.

**call fallback jitter-probe precedence** *precedence-value*

**no call fallback jitter-probe precedence** *precedence-value*

<b>Syntax Description</b>	<i>precedence-value</i>	Specifies the jitter-probe precedence. The valid range is from 0 to 6.
---------------------------	-------------------------	--

## call fallback jitter-probe priority-queue

To assign a priority queue, use the **call fallback jitter-probe priority-queue** command in global configuration mode. To return to default values, use the **no** form of this command.

**call fallback jitter-probe priority-queue**

**no call fallback jitter-probe priority-queue**

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

## call fallback key-chain

To specify use of Message Digest 5 (MD5) authentication for sending and receiving response time reporter (RTR) probes, use the **call fallback key-chain** command in global configuration mode. To disable MD5 use, use the **no** form of this command.

**call fallback key-chain** *name-of-chain*

**no call fallback key-chain** *name-of-chain*

<b>Syntax Description</b>	<i>name-of-chain</i>	Specifies the name of the chain. This line is to be alphanumeric and case-sensitive text.
---------------------------	----------------------	---

## call fallback map address-list

To specify the call fall back router to keep a cache table by IP addresses of distances for several destination peers sitting behind the router, use the **call fallback map address-list** command in global configuration mode. To restore the default values, use the **no** form of this command.

**call fallback map** *map target ip-address address-list ip-address1 ip-address2 ... ip-address7*

**no call fallback map** *map target ip-address address-list ip-address1 ip-address2 ... ip-address7*

Syntax Description		
<i>map</i>		Specifies the fall back map. The valid range is from 1 to 16.
<b>target</b> <i>ip-address</i>		Specifies the target IP address.
<i>ip-address1 ... ip-address7</i>		Lists the IP addresses that will be kept in the cache table. The maximum number of IP addresses is seven.

## call fallback map subnet

To configure the call fall back router to keep a cache table by subnet addresses of distances for several destination peers sitting behind the router, use the **call fallback map subnet** command in global configuration mode. To restore the default values, use the **no** form of this command.

```
call fallback map map target ip-address subnet ip-network netmask
```

```
no call fallback map map target ip-address subnet ip-network netmask
```

Syntax Description		
<i>map</i>		Specifies the fall back map. The valid range is from 1 to 16.
<b>target</b> <i>ip-address</i>		Specifies the target IP address.
<b>subnet</b> <i>ip-network</i>		Specifies the subnet IP address.
<i>netmask</i>		Specifies the network mask number.

## call fallback monitor

To enable the monitoring of destinations without call fall back to alternate dial peers, use the **call fallback monitor** command in global configuration mode. To disable monitoring without fall back, use the **no** form of this command.

```
call fallback monitor
```

```
no call fallback monitor
```

Syntax Description	
	This command has no arguments or keywords.

## call fallback probe-timeout

To set the timeout for a response time reporter (RTR) probe for call fall back purposes, use the **call fallback probe-timeout** command in global configuration command. To restore the default value, use the **no** form of this command.

```
call fallback probe-timeout seconds
```

```
no call fallback probe-timeout seconds
```

Syntax Description		
<i>seconds</i>		Specifies the interval in seconds. The valid range is from 1 to 2,147,483.

## call fallback threshold delay loss

To configure the call fall back threshold to use only packet delay and loss values, use the **call fallback threshold delay loss** command in global configuration mode. To restore the default value, use the **no** form of this command.

**call fallback threshold delay** *delay-value* **loss** *loss-value*

**no call fallback threshold delay** *delay-value* **loss** *loss-value*

Syntax Description		
<i>delay-value</i>		Sets the delay value. The valid range is from 1 to 2,147,483,647 milliseconds.
<i>loss-value</i>		Sets the loss value. The valid range is from 0 to 100 percent.

## call fallback threshold icpif

To configure call fallback to use the Impairment/Calculated Planning Impairment Factor (ICPIF) threshold, use the **call fallback threshold icpif** command in global configuration mode. To restore the default value, use the **no** form of this command.

**call fallback threshold icpif** *threshold-value*

**no call fallback threshold icpif** *threshold-value*

Syntax Description		
<i>threshold-value</i>		Sets the threshold value. The valid range is from 0 to 34.

## call rsvp-sync

To enable synchronization between Resource Reservation Protocol (RSVP) signaling and the voice signaling protocol, use the **call rsvp-sync** command in global configuration mode. To disable synchronization, use the **no** form of this command.

**call rsvp-sync**

**no call rsvp-sync**

Syntax Description	
	This command has no keywords or arguments.

## call rsvp-sync resv-timer

To set the timer on the terminating VoIP gateway for completing RSVP reservation setups, use the **call rsvp-sync resv-timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
call rsvp-sync resv-timer seconds
```

```
no call rsvp-sync resv-timer
```

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds in which the reservation setup must be completed, in both directions. The value range is from 1 to 60 seconds.
---------------------------	----------------	--

## call start

To force the H.323 Version 2 gateway to use fast connect or slow connect procedures for a dial peer, use the **call start** command in voice-class configuration mode. To restore the default condition, use the **no** form of this command.

```
call start {fast | slow | system}
```

```
no call start
```

<b>Syntax Description</b>	<b>fast</b>	Gateway uses H.323 Version 2 (fast connect) procedures.
	<b>slow</b>	Gateway uses H.323 Version 1 (slow connect) procedures.
	<b>system</b>	Gateway defaults to the voice service configuration that is defined using the <b>h323 call start</b> command in voice-service configuration mode.

## call-waiting

To enable call waiting, use the **call-waiting** command in interface configuration mode. To disable call waiting, use the **no** form of this command.

```
call-waiting
```

```
no call-waiting
```

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

## called-number (dial-peer)

To enable an incoming Voice over Frame Relay (VoFR) call leg to get bridged to the correct plain old telephone service (POTS) call leg when a static FRF.11 trunk connection is used, use the **called-number** command in dial peer configuration mode. To disable a static trunk connection, use the **no** form of this command.

**called-number** *string*

**no called-number**

---

### Syntax Description

<i>string</i>	A string of digits, including wildcards, that specifies the telephone number of the voice port dial peer.
---------------	---

---

## caller-id

To enable caller ID, use the **caller-id** command in dial peer configuration mode. To disable caller ID, use the **no** form of the command.

**caller-id**

**no caller-id**

---

### Syntax Description

This command has no arguments or keywords.

## caller-id alerting dsp-pre-alloc

To statically allocate a digital signal processor (DSP) resource for receiving caller ID information for on-hook (Type 1) Caller ID at a receiving Foreign Exchange Office (FXO) voice port, use the **caller-id alerting dsp-pre-alloc** command in voice-port configuration mode. To disable the command's effect, use the **no** form of this command.

**caller-id alerting dsp-pre-alloc**

**no caller-id alerting dsp-pre-alloc**

---

### Syntax Description

This command has no arguments or keywords.

## caller-id alerting line-reversal

To set the line-reversal alerting method for Caller-ID information for on-hook (Type 1) Caller ID at a sending Foreign Exchange Station (FXS) voice port, use the **caller-id alerting line-reversal** command in voice-port configuration mode. To disable the command's effect, use the **no** form of this command.

**caller-id alerting line-reversal**

**no caller-id alerting line-reversal**

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

## caller-id alerting pre-ring

To set a 250-millisecond pre-ring alerting method for caller ID information for on-hook (Type 1) Caller ID at a sending Foreign Exchange Station (FXS) voice port, use the **caller-id alerting pre-ring** command in voice-port configuration mode. To disable the command, use the **no** form of this command.

**caller-id alerting pre-ring**

**no caller-id alerting pre-ring**

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

## caller-id alerting ring

To set the ring-cycle method for receiving caller ID information for on-hook (Type 1) Caller ID at a receiving Foreign Exchange Office (FXO) or a sending Foreign Exchange Station (FXS) voice port, use the **caller-id alerting ring** command in voice-port configuration mode. To set the command to the default, use the **no** form of this command.

**caller-id alerting ring {1 | 2}**

**no caller-id alerting ring**

Syntax Description		
	1	Use this setting if your telephone service provider specifies it to provide caller ID alerting (display) after the first ring at the receiving station. This is the most common setting.
	2	Use this setting if your telephone service provider specifies it to provide caller ID alerting (display) after the second ring. This setting is used in Australia, where the caller ID information is sent following two short rings (double-pulse ring).

## caller-id attenuation

To set the attenuation for caller ID at a receiving Foreign Exchange Office (FXO) voice port, use the **caller-id attenuation** command in voice-port configuration mode. To set the command to the default, use the **no** form of this command.

**caller-id attenuation** [*attenuation*]

**no caller-id attenuation**

---

**Syntax Description***attenuation*Specifies the attenuation. Valid values are from 0 to 64.

---

## caller-id block

To request the blocking of the display of caller ID information at the far end of a call from calls originated at a Foreign Exchange Station (FXS) port, use the **caller-id block** command in voice-port configuration mode at the originating FXS voice port. To allow the display of caller ID information, use the **no** form of this command.

**caller-id block**

**no caller-id block**

---

**Syntax Description**

This command has no arguments or keywords.

## caller-id enable

To allow the sending or receiving of caller ID information, use the **caller-id enable** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or the receiving Foreign Exchange Office (FXO) voice port. To disable the sending or receiving of caller ID information, use the **no** form of this command, which also clears all other caller ID configuration settings for the voice port.

**caller-id enable**

**no caller-id enable**

---

**Syntax Description**

This command has no arguments or keywords.

## calling-number outbound

To specify automatic number identification (ANI) to be sent out when T1-channel associated signaling (T1-CAS) Feature Group-D-Exchange Access North American (FGD—EANA) is configured as the signaling type, use the **calling-number outbound** command in dial peer or voice-port configuration mode. To disable the **calling-number outbound** command, use **no** form of this command.

```
calling-number outbound { range string1 string2 | sequence string1... string5 | null }
```

```
no calling-number outbound { range string1 string2 | sequence string1 ... string5 | null }
```

Syntax Description		
<b>range</b>		Generates the sequence of ANI by rotating through the specified range ( <i>string1</i> to <i>string2</i> ).
<b>sequence</b>		Configures a sequence of discrete strings ( <i>string1... string5</i> ) to be passed out as ANI for successive calls using the peer.
<b>null</b>		Suppresses ANI. If used, no ANI will be passed when this dial peer is selected.
<i>string# ...</i>		Valid E.164 telephone number strings. Strings must be of equal length and cannot be more than 32-digits long.

## cap-list vfc

To add a voice codec overlay file to the capability file list, use the **cap-list vfc** command in global configuration mode. To disable a particular codec overlay file that has been added to the capability list, use the **no** form of this command.

```
cap-list filename vfc slot-number
```

```
no cap-list filename vfc slot-number
```

Syntax Description		
<i>filename</i>		Identifies the codec file stored in voice feature card (VFC) Flash memory.
<i>slot-number</i>		Identifies the slot where the VFC is installed. Valid values are 0, 1, and 2.

## card type

To configure the card type on the port adapter of the Cisco 7200 series routers router, use the **card type** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
card type { t1 | e1 } slot [bay]
```

```
no card type
```

Syntax Description		
<b>t1</b>		Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding.
<b>e1</b>		Specifies a wide-area digital transmission scheme used predominately in Europe that carries data at a rate of 2.048 Mbps.
<i>slot</i>		Slot number of the interface.
<i>bay</i>		(Optional) Card interface bay number in a slot (route/switch processor [RSP] platform only).

## ccs connect (interface)

To configure a common channel signaling (CCS) connection on an interface configured to support CCS frame forwarding, use the **ccs connect** command in interface configuration mode. To disable the CCS connection on the interface, use the **no** form of this command.

```
ccs connect {serial | atm} number [dlci | pvc vpi/vci | pvc name] [cidnumber]
```

```
no ccs connect {serial | atm} number [dlci | pvc vpi/vci | pvc name] [cidnumber]
```

Syntax Description		
<b>serial</b>		Makes a serial CCS connection for Frame Relay.
<b>atm</b>		Makes an ATM CCS connection for ATM.
<i>dlci</i>		(Optional) Specifies the data link connection identifier (DLCI) number.
<b>pvc vpi/vci</b>		(Optional) Specifies the permanent virtual circuit (PVC) virtual path identifier or virtual channel identifier. Acceptable values are from 0 to 255; the slash is required.
<b>pvc name</b>		(Optional) Specifies the PVC string that names the PVC for recognition.
<i>cidnumber</i>		(Optional) If you have executed the <b>ccs encap frf11</b> command, the <i>cidnumber</i> option allows you to specify any channel identification (CID) number from 5 to 255.

## ccs connect (controller)

To configure a common channel signaling (CCS) connection on an interface configured to support CCS frame forwarding, use the **ccs connect** command in controller configuration mode. To disable the CCS connection on the interface, use the **no** form of this command.

```
ccs connect {serial | atm} number [dlci | pvc vpi/vci | pvc name] [cidnumber]
```

```
no ccs connect {serial | atm} number [dlci | pvc vpi/vci | pvc name] [cidnumber]
```

Syntax Description		
<b>serial</b>		Makes a serial CCS connection for Frame Relay.
<b>atm</b>		Makes an ATM CCS connection.
<i>dlci</i>		(Optional) Specifies the data-link connection identifier (DLCI) number.

<b>pvc</b> <i>vpi/vci</i>	(Optional) Specifies the permanent virtual circuit (PVC) virtual path identifier or virtual channel identifier. Acceptable values are from 0 to 255; the slash is required.
<b>pvc</b> <i>name</i>	(Optional) Specifies the PVC string that names the PVC for recognition.
<i>cidnumber</i>	(Optional) If you have executed the <b>ccs encap frf11</b> command, the <i>cidnumber</i> option allows you to specify any channel identification (CID) number from 5 to 255.

## ccs encap frf11

To configure the common channel signaling (CCS) packet encapsulation format for FRF.11, use the **ccs encap frf11** command in interface configuration mode. To disable ccs encapsulation for FRF11, use the **no** form of this command.

```
ccs encap frf11
```

```
no ccs encap frf11
```

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

## ces cell-loss-integration-period

To set the circuit emulation service (CES) cell-loss integration period, use the **ces cell-loss-integration-period** command in interface configuration mode. To delete the cell-loss integration period, use the **no** form of this command.

```
ces cell-loss-integration-period period
```

```
no ces cell-loss-integration-period period
```

**Syntax Description**

<i>period</i>	Time, in milliseconds, for the cell-loss integration period. Possible values are from 1 to MAXINT.
---------------	--

## ces-clock

To configure the clock for the CES interface, use the **ces-clock** command in controller configuration mode. To disable the ces clock, use the **no** form of this command.

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

```
no ces-clock {adaptive | srts | synchronous}
```

<b>Syntax Description</b>	<b>adaptive</b>	Adjusts output clock on a received ATM Adaptation Layer 1 (AAL1) on first-in, first-out 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 clockmode synchronous

To configure the ATM circuit emulation service (CES) synchronous clock mode, use the **ces clockmode synchronous** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ces clockmode synchronous**

**no ces clockmode synchronous**

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

## ces connect

To map the circuit emulation service (CES) service to an ATM permanent virtual circuit (PVC) on the Cisco MC3810 multiservice concentrator, use the **ces connect** command in interface configuration mode. To delete the CES map to the ATM PVC, use the **no** form of this command.

**ces connect** *atm-interface* **pvc** {*name* | [*vpi*]/*vci*}

**no ces connect** *atm-interface* **pvc** [*name* | [*vpi*]/*vci*]

<b>Syntax Description</b>	<i>atm-interface</i>	Number of the ATM interface. The only valid option on the Cisco MC3810 multiservice concentrator is ATM0.
	<b>pvc</b>	Specifies that the connection is to an ATM PVC.
	<i>name</i>	The name of the ATM PVC.
	<i>vpi</i> /	(Optional) The virtual path identifier value.
	<i>vci</i>	The virtual channel identifier value.

## ces initial-delay

To configure the size of the receive buffer of a circuit emulation service (CES) circuit, use the **ces initial-delay** command in interface configuration mode. To remove the initial-delay value, use the **no** form of this command.

**ces initial-delay** *bytes*

**no ces initial-delay** *bytes*

<b>Syntax Description</b>	<i>bytes</i>	The size of the receive buffer of the CES circuit. The valid range is from 1 to 16,000 bytes. This command is used to accommodate cell jitter on the network. Bytes received from the ATM network are buffered by this amount before being sent to the CES port.
---------------------------	--------------	--

## ces max-buf-size

To configure the transmit buffer of a circuit emulation service (CES) circuit, use the **ces max-buf-size** command in interface configuration mode. To delete the CES transmit buffer size, use the **no** form of this command.

**ces max-buf-size** *size*

**no ces max-buf-size** *size*

<b>Syntax Description</b>	<i>size</i>	Maximum size of the transmit buffer for the CES. Possible values are from 80 to 1520.
---------------------------	-------------	---

## ces service

To configure the ATM circuit emulation service (CES) type, use the **ces service** command in interface configuration mode. To disable the ATM CES service type, use the **no** form of this command.

**ces service structured**

**no ces service structured**

<b>Syntax Description</b>	<b>structured</b>	Specifies that the ATM CES type is structured. Structured is the only option supported in this release.
---------------------------	-------------------	---

## clear call fallback cache

To clear the current Impairment/Calculated Planning Impairment Factor (ICPIF) estimates for all IP addresses or for a specific IP address in the cache, use the **clear call fallback cache** command in EXEC mode.

```
clear call fallback cache [ip-address]
```

<b>Syntax Description</b>	<i>ip-address</i>	(Optional) Specifies the target IP address.
---------------------------	-------------------	---

## clear call fallback stats

To clear the call fall back statistics, use the **clear call fallback stats** command in EXEC mode.

```
clear call fallback stats
```

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

## clear controllers call-counters

To clear the system's DS0's High Water Marks (HWM) and all individual controller statistics, enter the **clear controllers call-counters** command in privileged EXEC mode.

```
clear controllers {t1 | e1} number call-counters [system-hwm | all]
```

<b>Syntax Description</b>	<b>t1   e1</b>	Specifies the type of controller. If the <b>t1</b> or <b>e1</b> keyword is specified, then the command acts on the individual controller specified in <i>number</i> . In this case, the additional options of <b>system-hwm</b> or <b>all</b> will not be available.
	<i>number</i>	Clears an individual controller. Select the shelf (for Cisco ASRouters) /slot/port number in the following format: <i>shelf/slot/port</i> .
	<b>system-hwm</b>	(Optional) Clears the system's HWM only (not the individual controllers).
	<b>all</b>	(Optional) Clears all HWMs (individual DS0s and the system total HWM). This keyword clears <i>all</i> controller call-counters, including the individual controller time slots' time in use and the number of calls on those time slots since the last reset was done using the <b>clear controllers</b> command on that controller.

## clear csm-statistics modem

To clear the call switching module (CSM) statistics for a modem or group of modems, use the **clear csm-statistics modem** command in privileged EXEC mode.

```
clear csm-statistics modem [slot/port | modem-group-number]
```

<b>Syntax Description</b>	<i>slot/port</i>	(Optional) Identifies the location (and thereby the identity) of a specific modem.
	<i>modem-group-number</i>	(Optional) Designates a defined modem group.

## clear csm-statistics voice

To clear the call switching module (CSM) statistics for a particular or for all digital signal processor (DSP) channels, use the **clear csm-statistics voice** command in privileged EXEC mode.

```
clear csm-statistics voice [slot/dspm/dsp/dsp-channel]
```

<b>Syntax Description</b>	<i>slot/dspm/dsp/dsp-channel</i>	(Optional) Identifies the location of a particular DSP channel.
---------------------------	----------------------------------	---

## clear h323 gatekeeper call

To force a disconnect of a specific call or of all calls active on a particular gatekeeper, use the **clear h323 gatekeeper call** command in privileged EXEC mode.

```
clear h323 gatekeeper call {all | local-callID local-callID}
```

<b>Syntax Description</b>	<b>all</b>	Forces all active calls currently associated with this gatekeeper to be disconnected.
	<b>local-callID</b>	Forces a single active call associated with this gatekeeper to be disconnected.
	<i>local-callID</i>	Specifies the local call identification number (CallID) that identifies the call to be disconnected.

## clear mgcp statistics

To reset the Media Gateway Control Protocol (MGCP) statistical counters, use the **clear mgcp statistics** command in privileged EXEC mode.

```
clear mgcp statistics
```

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

## clear sgcp statistics

To clear all Simple Gateway Control Protocol (SGCP) statistics, use the **clear sgcp statistics** command in privileged EXEC mode.

**clear sgcp statistics**

---

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

## clear voice port

To clear voice port calls in progress, use the **clear voice port** command in privileged EXEC mode.

**clear voice port** [*slot/port*]

---

**Syntax Description** *slot/port* (Optional) The voice port slot number and port number. If you do not specify a voice port, all calls on all voice ports are cleared.

---

## clock rate line

To configure the line clock rate for serial ports 0 or 1 in DTE mode, use the **clock rate line** command in interface configuration mode. To cancel the clock rate line value, use the **no** form of this command.

**clock rate line** *rate*

**no clock rate line** *rate*

---

**Syntax Description** *rate* Network clock line rate, in bits per second. The range is from 56 kbps to 2048 kbps. The value entered should be a multiple of 8000 of the value set for the **network-clock base-rate** command. There is no default rate.

---

## clock rate network-clock

To configure the network clock speed for serial ports 0 or 1 in DCE mode, use the **clock rate network-clock** command in interface configuration mode. To cancel the network clock speed value, use the **no** form of this command.

**clock rate network-clock** *rate*

**no clock rate network-clock** *rate*

<b>Syntax Description</b>	<i>rate</i>	Network clock speed, in bits per second. The range is from 56 kbps to 2048 kbps. The value entered should be a multiple of the value set for the <b>network-clock base-rate</b> command. There is no default rate.
---------------------------	-------------	--

## clock-select

To establish the sources and priorities of the requisite clocking signals for the OC-3/STM-1 ATM Circuit Emulation Service network module, use the **clock-select** command in CES configuration mode.

**clock-select** *priority-number interface slot/port*

<b>Syntax Description</b>	<i>priority-number</i>	Priority of the clock source. Values are 1 (high priority) to 4 (low priority).
	<i>interface</i>	Specifies the interface to supply the clock source.
	<i>slot/port</i>	Backplane slot number and port number on the interface.

## codec (dial-peer)

To specify the voice coder rate of speech for a dial peer, use the **codec** command in dial peer configuration mode. To reset the default value, use the **no** form of this command.

### Cisco 2600 and 3600 Series Routers and Cisco AS5300 and AS5800 Universal Access Servers

```
codec codec {clear channel | g711alaw | g711ulaw | g723ar53 | g723ar63 | g723r53 | g723r63 |
g726r16 | g726r24 | g726r32 | g726r53 | g726r63 | g728 | g729abr8 | g729ar8 | g729br8 |
g729r8 | gsmefr | gsmfr} [bytes payload_size]
```

```
no codec {clear channel | g711alaw | g711ulaw | g723ar53 | g723ar63 | g723r53 | g723r63 |
g726r16 | g726r24 | g726r32 | g726r53 | g726r63 | g728 | g729abr8 | g729ar8 | g729br8 |
g729r8 | gsmefr | gsmfr} [bytes payload_size]
```

### Cisco MC3810 Multiservice Concentrators

```
codec codec {clear-channel | g711alaw | g711ulaw | g723ar53 | g723ar63 | g723r53 | g723r63 |
g726r16 | g726r24 | g726r32 | g728 | g729abr8 | g729ar8 | g729br8 | g729r8 | gsmefr | gsmfr}
[bytes payload_size]
```

```
no codec {clear-channel | g711alaw | g711ulaw | g723ar53 | g723ar63 | g723r53 | g723r63 |
g726r16 | g726r24 | g726r32 | g728 | g729abr8 | g729ar8 | g729br8 | g729r8 | gsmefr | gsmfr}
[bytes payload_size]
```

**Syntax Description****For the Cisco 2600 and 3600 Series Routers and Cisco AS5300 and AS5800 Universal Access Servers**

<b>codec</b>	Sets the codec options that you can use when you execute this command.
<i>codec</i>	Codec options are as follows: <ul style="list-style-type: none"> <li>• <b>clear-channel</b>—Clear channel at 64,000 bits per second (bps).</li> <li>• <b>g711alaw</b>—G.711 a-Law at 64,000 bits per second.</li> <li>• <b>g711ulaw</b>—G.711 u-Law at 64,000 bps.</li> <li>• <b>g723ar53</b>—G.723.1 Annex A at 5300 bps.</li> <li>• <b>g723ar63</b>—G.723.1 Annex A at 6300 bps.</li> <li>• <b>g723r53</b>—G.723.1 at 5300 bps.</li> <li>• <b>g723r63</b>—G.723.1 at 6300 bps.</li> <li>• <b>g726r16</b>—G.726 at 16,000 bps.</li> <li>• <b>g726r24</b>—G.726 at 24,000 bps.</li> <li>• <b>g726r32</b>—G.726 at 32,000 bps.</li> <li>• <b>g728</b>—G.728 at 16,000 bps.</li> <li>• <b>g729abr8</b>—G.729 Annex A and B at 8000 bps.</li> <li>• <b>g729ar8</b>—G.729 Annex A at 8000 bps.</li> <li>• <b>g729br8</b>—G.729 Annex B at 8000 bps.</li> <li>• <b>g729r8</b>—G.729 at 8000 bps. This is the default codec.</li> <li>• <b>gsmefr</b>—Global System for Mobile Communications Enhanced Rate Codecs (GSMEFR) at 12,200 bps.</li> <li>• <b>gsmfr</b>—Global System for Mobile Communications Full Rate (GSMFR) at 13200 bps.</li> </ul>
<b>bytes</b>	(Optional) Specifies the number of bytes in the voice payload of each frame.
<i>payload_size</i>	(Optional) The number of bytes in the voice payload of each frame. See Table 6 for valid entries and default values.

**For the Cisco MC3810 Multiservice Concentrators**

<b>codec</b>	Sets the codec options that you can use when you execute this command.
<i>codec</i>	Codec options are as follows: <ul style="list-style-type: none"> <li>• <b>clear-channel</b>—Clear channel at 64,000 bits per second (bps).</li> <li>• <b>g711alaw</b>—G.711 a-Law at 64,000 bits per second.</li> <li>• <b>g711ulaw</b>—G.711 u-Law at 64,000 bps.</li> <li>• <b>g723ar53</b>—G.723.1 Annex A at 5300 bps.</li> <li>• <b>g723ar63</b>—G.723.1 Annex A at 6300 bps.</li> <li>• <b>g723r53</b>—G.723.1 at 5300 bps.</li> <li>• <b>g723r63</b>—G.723.1 at 6300 bps.</li> <li>• <b>g726r16</b>—G.726 at 16,000 bps.</li> <li>• <b>g726r24</b>—G.726 at 24,000 bps.</li> <li>• <b>g726r32</b>—G.726 at 32,000 bps.</li> <li>• <b>g728</b>—G.728 at 16,000 bps.</li> <li>• <b>g729abr8</b>—G.729 Annex A and B at 8000 bps.</li> <li>• <b>g729ar8</b>—G.729 Annex A at 8000 bps.</li> <li>• <b>g729br8</b>—G.729 Annex B at 8000 bps.</li> <li>• <b>g729r8</b>—G.729 at 8000 bps. This is the default codec.</li> <li>• <b>gsmeifr</b>—Global System for Mobile Communications Enhanced Rate Codecs (GSMEFR) at 12,200 bps.</li> <li>• <b>gsmfr</b>—Global System for Mobile Communications Full Rate (GSMFR) at 13,200 bps.</li> </ul>
<i>bytes</i>	(Optional) Specifies the number of bytes in the voice payload of each frame.
<i>payload_size</i>	(Optional) The number of bytes in the voice payload of each frame. See Table 6 for valid entries and default values.

**Table 6 Voice Payload-per-Frame Options and Defaults**

<b>Codec</b>	<b>Protocol</b>	<b>Voice Payload Options (in bytes)</b>	<b>Default Voice Payload (in bytes)</b>
<b>g711alaw</b>	VoIP	80, 160	160
<b>g711ulaw</b>	VoFR	40 to 240 in multiples of 40	240
	VoATM	40 to 240 in multiples of 40	240
<b>g723ar53</b> <b>g723r53</b>	VoIP	20 to 220 in multiples of 20	20
	VoFR	20 to 240 in multiples of 20	20
	VoATM	20 to 240 in multiples of 20	20
<b>g723ar63</b> <b>g723r63</b>	VoIP	24 to 216 in multiples of 24	24
	VoFR	24 to 240 in multiples of 24	24
	VoATM	24 to 240 in multiples of 24	24

**Table 6** Voice Payload-per-Frame Options and Defaults (continued)

Codec	Protocol	Voice Payload Options (in bytes)	Default Voice Payload (in bytes)
<b>g726r16</b>	VoIP	20 to 220 in multiples of 20	40
	VoFR	10 to 240 in multiples of 10	60
	VoATM	10 to 240 in multiples of 10	60
<b>g726r24</b>	VoIP	30 to 210 in multiples of 30	60
	VoFR	15 to 240 in multiples of 15	90
	VoATM	30 to 240 in multiples of 15	90
<b>g726r32</b>	VoIP	40 to 200 in multiples of 40	80
	VoFR	20 to 240 in multiples of 20	120
	VoATM	40 to 240 in multiples of 20	120
<b>g728</b>	VoIP	10 to 230 in multiples of 10	40
	VoFR	10 to 240 in multiples of 10	60
	VoATM	10 to 240 in multiples of 10	60
<b>g729abr8</b>	VoIP	10 to 230 in multiples of 10	20
<b>g729ar8</b>	VoFR	10 to 240 in multiples of 10	30
<b>g729br8</b>	VoATM	10 to 240 in multiples of 10	30
<b>g729r8</b>			

## codec (dsp)

To specify call density and codec complexity based on a particular codec standard, use the **codec** command in DSP interface dsp farm mode. To reset the card type to the default, use the **no** form of the command.

**codec** { **high** | **med** }

**no codec** { **high** | **med** }

### Syntax Description

high	Specifies high complexity: two channels of any mix of codec.
med	Specifies medium complexity: four channels of g711/g726/g729a/fax.

## codec (voice-port)

The **codec** command in voice-port configuration mode on the Cisco MC3810 multiservice concentrator that was first supported in Cisco IOS Release 11.3(1)MA is no longer supported, beginning with Cisco IOS Release 12.2. Configure the codec value using the **codec** dial peer configuration command.

## codec aal2-profile

To set the codec profile for a digital signal processor (DSP) on a per-call basis, enter the **codec aal2-profile** command in dial peer configuration mode. To restore the default value, use the **no** form of the command.

```
codec aal2-profile {ituf | atmf | custom} profile-number codec
```

```
no codec aal2-profile
```

### Syntax Description

<b>ituf</b>	Specifies the <i>profile-number</i> as an ITU-T type.
<b>atmf</b>	Specifies the <i>profile-number</i> as an ATMF type.
<b>custom</b>	Specifies the <i>profile-number</i> as a custom type.
<i>profile-number</i>	The available <i>profile-number</i> selections depend on the profile type. For ITU-T: <ul style="list-style-type: none"> <li>• 1 = G.711ulaw</li> <li>• 2 = G.711ulaw with silence insertion descriptor (SID)</li> <li>• 7 = G.711ulaw and G.729ar8</li> </ul> For ATMF: None. ATMF is not supported. For custom: <ul style="list-style-type: none"> <li>• 100 = G.711ulaw and G.726r32</li> <li>• 110 = G.711ulaw, G.726r32, and G.729ar8</li> </ul>
<i>codec</i>	Enter one codec for the DSP. The possible <i>codec</i> entries depend on the <i>profile-number</i> . The valid entries are as follows: <ul style="list-style-type: none"> <li>• For ITU 1—g711ulaw</li> <li>• For ITU 2—g711ulaw</li> <li>• For ITU 7—g711ulaw or g729ar8</li> <li>• For custom 100—g711ulaw or g726r32</li> <li>• For custom 110—g711ulaw or g726r32 or g729ar8</li> </ul>

## codec complexity

To specify call density and codec complexity based on the codec standard you are using, use the **codec complexity** command in voice-card configuration mode. To reset the voice card to the default, use the **no** form of this command.

```
codec complexity {high | medium}
```

```
no codec complexity
```

Syntax Description	high	Each digital signal processor (DSP) supports two voice channels encoded in any of the following formats:
		<ul style="list-style-type: none"> <li>• <b>g711alaw</b>—G.711 A-law 64,000 bps.</li> <li>• <b>g711ulaw</b>—G.711 U-law 64,000 bps.</li> <li>• <b>g723ar53</b>—G.723.1 Annex A 5300 bps.</li> <li>• <b>g723ar63</b>—G.723.1 Annex A 6300 bps.</li> <li>• <b>g723r53</b>—G.723.1 5300 bps.</li> <li>• <b>g723r63</b>—G.723.1 6300 bps.</li> <li>• <b>g723r16</b>—G.726 16,000 bps.</li> <li>• <b>g726r24</b>—G.726 24,000 bps.</li> <li>• <b>g726r32</b>—G.726 32,000 bps.</li> <li>• <b>g728</b>—G.728 16,000 bps.</li> <li>• <b>g729r8</b>—G.729 8000 bps. (default)</li> <li>• <b>g729br8</b>—G.729 Annex B 8000 bps.</li> <li>• <b>fax relay</b></li> </ul>
	medium	Each DSP supports four voice channels encoded in any of the following formats:
		<ul style="list-style-type: none"> <li>• <b>g711alaw</b>—G.711 a-Law 64,000 bps.</li> <li>• <b>g711ulaw</b>—G.711 u-Law 64,000 bps.</li> <li>• <b>g726r16</b>—G.726 16,000 bps.</li> <li>• <b>g726r24</b>—G.726 24,000 bps.</li> <li>• <b>g726r32</b>—G.726 32,000 bps.</li> <li>• <b>g729r8</b>—G.729 Annex A 8000 bps.</li> <li>• <b>G729br8</b>—G.729 Annex B with Annex A 8000 bps.</li> <li>• <b>fax relay</b></li> </ul>

## codec preference

To specify a list of preferred codecs to use on a dial peer, use the **codec preference** command in voice-class configuration mode. To disable this functionality, use the **no** form of this command.

**codec preference** *value codec\_type* [**bytes** *payload-size*]

**no codec preference** *value codec\_type*

<b>Syntax Description</b>	<i>value</i>	Specifies the order of preference, with 1 being the most preferred and 14 being the least preferred.
	<i>codec_type</i>	Specifies the codec preferred. <ul style="list-style-type: none"> <li>• <b>clear-channel</b>—Clear Channel 64,000 bps</li> <li>• <b>g711alaw</b>—G.711 A Law 64,000 bps</li> <li>• <b>g711ulaw</b>—G.711 u Law 64,000 bps</li> <li>• <b>g723ar53</b>—G.723.1 ANNEX-A 5,300 bps</li> <li>• <b>g723ar63</b>—G.723.1 ANNEX-A 6,300 bps</li> <li>• <b>g723r53</b>—G.723.1 5,300 bps</li> <li>• <b>g723r63</b>—G.723.1 6,300 bps</li> <li>• <b>g726r16</b>—G.726 16,000 bps</li> <li>• <b>g726r24</b>—G.726 24,000 bps</li> <li>• <b>g726r32</b>—G.726 32,000 bps</li> <li>• <b>g728</b>—G.728 16,000 bps</li> <li>• <b>g729abr8</b>—G.729 ANNEX-A &amp; B 8,000 bps</li> <li>• <b>g729br8</b>—G.729 ANNEX-B 8,000 bps</li> <li>• <b>g729r8</b>—G.729 8000 bps</li> <li>• <b>gsmefr</b>—Global System for Mobile Communications Enhanced Full Rate (GSMEFR) 12,200 bps</li> <li>• <b>gsmfr</b>—Global System for Mobile Communications (GSM) Full Rate (GSMFR) 13,200 bps</li> </ul>
	<b>bytes</b>	(Optional) Specifies that the size of the voice frame is in bytes.
	<i>payload-size</i>	(Optional) Number of bytes you specify as the voice payload of each frame. Values depend on the codec type and the packet voice protocol.

## comfort-noise

To generate background noise to fill silent gaps during calls if voice activity detection (VAD) is activated, use the **comfort-noise** command in voice-port configuration mode. To provide silence when the remote party is not speaking and VAD is enabled at the remote end of the connection, use the **no** form of this command.

**comfort-noise**

**no comfort-noise**

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

## compand-type

To specify the companding standard used to convert between analog and digital signals in pulse code modulation (PCM) systems, use the **compand-type** command in voice-port configuration mode. To disable the compand type, use the **no** form of this command.

```
compand-type { u-law | a-law }
```

```
no compand-type { u-law | a-law }
```

### Syntax Description

<b>u-law</b>	Specifies the North American U-law ITU-T PCM encoding standard.
<b>a-law</b>	Specifies the European a-law ITU-T PCM encoding standard.

## condition

To manipulate the signaling format bit-pattern for all voice signaling types, use the **condition** command in voice-port configuration mode. To turn off conditioning on the voice port, use the **no** form of this command.

```
condition { tx-a-bit | tx-b-bit | tx-c-bit | tx-d-bit } { rx-a-bit | rx-b-bit | rx-c-bit | rx-d-bit }
{ on | off | invert }
```

```
no condition { tx-a-bit | tx-b-bit | tx-c-bit | tx-d-bit } { rx-a-bit | rx-b-bit | rx-c-bit | rx-d-bit }
{ on | off | invert }
```

### Syntax Description

<b>tx-a-bit</b>	Sends A bit.
<b>tx-b-bit</b>	Sends B bit.
<b>tx-c-bit</b>	Sends C bit.
<b>tx-d-bit</b>	Sends D bit.
<b>rx-a-bit</b>	Receives A bit.
<b>rx-b-bit</b>	Receives B bit.
<b>rx-c-bit</b>	Receives C bit.
<b>rx-d-bit</b>	Receives D bit.
<b>on</b>	Forces the bit state to be 1.
<b>off</b>	Forces the bit state to be 0.
<b>invert</b>	Inverts the bit state.

## connect (atm)

To define connections between T1 or E1 controller ports and the ATM interface, enter the **connect** command in global configuration mode. Use the no form of this command to restore the default values.

```
connect id atm slot/port-1 {name of PVC/SVC | vpi/vci} {T1 | E1} slot/port-2 TDM-group-number
```

```
no connect id atm slot/port-1 {name of PVC/SVC | vpi/vci} {T1 | E1} slot/port-2  
TDM-group-number
```

### Syntax Description

<i>id</i>	A name for this connection.
<b>atm</b>	Specifies the ATM interface.
<i>slot/port-1</i>	The location of the ATM controller to be connected.
<i>name of PVC/SVC</i>	Specifies the permanent or switched virtual circuit.
<i>vpi/vci</i>	Specifies a virtual path identifier (VPI) and virtual channel identifier (VCI).
<b>T1</b>	Specifies a T1 port.
<b>E1</b>	Specifies an E1 port.
<i>slot/port-2</i>	The location of the T1 or E1 controller to be connected.
<i>TDM-group-number</i>	The number identifier of the time-division multiplexing (TDM) group associated with the T1 or E1 controller port and created by using the <b>tdm-group</b> command. Valid values are from 0 to 23 for T1 and from 0 to 30 for E1.

## connect (drop-and-insert)

To define connections among T1 or E1 controller ports for drop-and-insert (also called TDM cross-connect), use the **connect** command in global configuration mode. To restore default values, use the **no** form of this command.

```
connect id {t1 | e1} slot/port-1 tdm-group-no-1 {t1 | e1} slot/port-2 tdm-group-no-2
```

```
no connect id {t1 | e1} slot/port-1 tdm-group-no-1 {t1 | e1} slot/port-2 tdm-group-no-2
```

### Syntax Description

<i>id</i>	A name for this connection.
<b>t1</b>	Specifies a T1 port.
<b>e1</b>	Specifies an E1 port.
<i>slot/port-1</i>	The location of the first T1 or E1 controller to be connected. Valid values for <i>slot</i> and <i>port</i> are 0 and 1.
<i>tdm-group-no-1</i>	The number identifier of the time-division multiplexing (TDM) group associated with the first T1 or E1 controller port and created by using the <b>tdm-group</b> command. Valid values are from 0 to 23 for T1 and from 0 to 30 for E1.

<i>slot/port-2</i>	The location of the second T1 or E1 controller port to be connected. Valid values for <i>slot</i> are from 0 to 5, depending on the platform. Valid values for <i>port</i> are 0 to 3, depending on the platform and the presence of a network module.
<i>tdm-group-no-2</i>	The number identifier of the time-division multiplexing (TDM) group associated with the second T1 or E1 controller and created by using the <b>tdm-group</b> command. Valid values are from 0 to 23 for T1 and from 0 to 30 for E1.

## connect (global)

This command, created for the Cisco MC3810-IGX Interworking feature in Cisco IOS Release 12.0(2)T, is not supported in Cisco IOS Release 12.2.

## connect voice

This command, created for the Cisco MC3810-IGX Interworking feature in Cisco IOS Release 12.0(2)T, is not supported in Cisco IOS Release 12.2.

## connection

To specify a connection mode for a voice port, use the **connection** command in voice-port configuration mode. To disable the selected connection mode, use the **no** form of this command.

**connection** {**plar** | **tie-line** | **plar-opx**} *digits* | {**trunk** *digits* [**answer-mode**]}

**no connection** {**plar** | **tie-line** | **plar-opx**} *digits* | {**trunk** *digits* [**answer-mode**]}

Syntax Description		
<b>plar</b>	Specifies a private line automatic ringdown (PLAR) connection. PLAR is an autodialing mechanism that permanently associates a voice interface with a far-end voice interface, allowing call completion to a specific telephone number or PBX without dialing. When the calling telephone goes off-hook, a predefined network dial peer is automatically matched, which sets up a call to the destination telephone or PBX.	
<b>tie-line</b>	Specifies a connection that emulates a temporary tie-line trunk to a private branch exchange (PBX). A tie-line connection is automatically set up for each call and torn down when the call ends.	
<b>plar-opx</b>	Specifies a PLAR off-premises extension (OPX) connection. Using this option, the local voice port provides a local response before the remote voice port receives an answer. On Foreign Exchange Office (FXO) interfaces, the voice port will not answer until the remote side has answered.	
<i>digits</i>	Specifies the destination telephone number. Valid entries are any series of digits that specify the E.164 telephone number.	

<b>trunk</b>	Specifies a connection that emulates a permanent trunk connection to a PBX. A trunk connection remains permanent in the absence of any active calls.
<b>answer-mode</b>	(Optional) Specifies that the router should not attempt to initiate a trunk connection but should wait for an incoming call before establishing the trunk. Used only with the <b>trunk</b> keyword.

## connection-timeout

To configure the time in seconds for which a connection is maintained after completion of a communication exchange, enter the **connection-timeout** command in settlement configuration mode. To return to the default value of this command, use the **no** form of this command to reset.

**connection timeout** *number*

**no connection timeout** *number*

<b>Syntax Description</b>	<i>number</i>	Time (in seconds) for which a connection is maintained after the communication exchange is completed. Values can range from 0 to 86,400 seconds; 0 means that the connection does not timeout.
---------------------------	---------------	--

## copy flash vfc

To copy a new version of VCWare from the Cisco AS5300 universal access server motherboard to voice feature card (VFC) Flash memory, use the **copy flash vfc** command in privileged EXEC mode.

**copy flash vfc** *slot-number*

<b>Syntax Description</b>	<i>slot-number</i>	Slot on the Cisco AS5300 universal access server in which the VFC is installed. Valid entries are from 0 to 2.
---------------------------	--------------------	--

## copy tftp vfc

To copy a new version of VCWare from a TFTP server to voice feature card (VFC) Flash memory, use the **copy tftp vfc** command in privileged EXEC mode.

**copy tftp vfc** *slot-number*

<b>Syntax Description</b>	<i>slot-number</i>	Slot on the Cisco AS5300 universal access server in which the VFC is installed. Valid entries are from 0 to 2.
---------------------------	--------------------	--

# cptone

To specify a regional analog voice interface-related tone, ring, and cadence setting, use the **cptone** command in voice-port configuration mode. To disable the selected tone, use the **no** form of this command.

**cptone** {*locale*}

**no cptone** {*locale*}

## Syntax Description

<i>locale</i>	Specifies an analog voice interface-related default tone, ring, and cadence setting for a specified country (for ISDN PRI and E1 R2 signaling). Keywords for the argument <i>locale</i> are contained in Table 7. Keywords for ISDN PRI signaling are contained in Table 8.  The Cisco 2600 and 3600 series routers and the Cisco MC3810 multiservice concentrator comply with the ISO 3166 country name standards, which use a two-letter code to represent a country.
---------------	---

**Table 7** *cptone locale* Argument Values

Argument Value	Country
<b>ar</b>	Argentina
<b>au</b>	Australia
<b>at</b>	Austria
<b>be</b>	Belgium
<b>br</b>	Brazil
<b>ca</b>	Canada
<b>cn</b>	China
<b>co</b>	Colombia
<b>cz</b>	Czech Republic
<b>dk</b>	Denmark
<b>fi</b>	Finland
<b>fr</b>	France
<b>de</b>	Germany
<b>gb</b>	Great Britain
<b>gr</b>	Greece
<b>hk</b>	Hong Kong
<b>hu</b>	Hungary
<b>is</b>	Iceland
<b>in</b>	India
<b>id</b>	Indonesia
<b>ie</b>	Ireland

**Table 7** *cptone locale Argument Values (continued)*

Argument Value	Country
il	Israel
it	Italy
jp	Japan
kr	Korea Republic
lu	Luxembourg
my	Malaysia
mx	Mexico
nl	Netherlands
nz	New Zealand
no	Norway
pe	Peru
ph	Philippines
pl	Poland
pt	Portugal
ru	Russian Federation
sg	Singapore
sk	Slovakia
si	Slovenia
za	South Africa
es	Spain
se	Sweden
ch	Switzerland
tw	Taiwan
th	Thailand
tr	Turkey
gb	Great Britain
us	United States
ve	Venezuela

**Table 8** *cptone locale Argument Values for ISDN PRI Signaling*

Argument Value	Description
australia	Specifies an analog voice interface-related default tone, ring, and cadence setting for Australia.
brazil	Specifies an analog voice interface-related default tone, ring, and cadence setting for Brazil.

**Table 8** *cptone locale Argument Values for ISDN PRI Signaling (continued)*

Argument Value	Description
<b>china</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for China.
<b>finland</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for Finland.
<b>france</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for France.
<b>germany</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for Germany.
<b>japan</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for Japan.
<b>northamerica</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for North America.
<b>sweden</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for Sweden.
<b>unitedkingdom</b>	Specifies an analog voice interface-related default tone, ring, and cadence setting for the United Kingdom.

## cross-connect

To cross-connect two groups of digital signal level 0s (DS0s) from two controllers on the Cisco MC3810 multiservice concentrator or to cross-connect the Universal I/O (UIO) serial port for pass-through traffic to a trunk controller, use the **cross-connect** command in global configuration mode. To remove the cross-connect function for the given controller, use the **no** form of this command.

### Pass-Through Traffic Between Two Controllers

```
cross-connect id controller-1 tdm-group-no-1 controller-2 tdm-group-no-2
```

```
no cross-connect id controller-1 tdm-group-no-1 controller-2 tdm-group-no-2
```

### Pass-Through Traffic from a UIO Serial Port to a Trunk Controller

```
cross-connect id interface-serial controller tdm-group-no
```

```
no cross-connect id interface-serial controller tdm-group-no
```



#### Note

The UIO serial port is either serial port 0 or 1.

### Syntax Description

#### Pass-Through Between Two Controllers

<i>id</i>	Unique identification (ID) assigned to this cross-connection. The valid range is from 0 to 31.
<i>controller-1</i>	Type of the first controller (T1 0, T1 1, or E1)

<i>tdm-group-no-1</i>	Time-division multiplexing (TDM) group number assigned to the first controller.
<i>controller-2</i>	Type of the second controller (T1, E1 0, or E1 1).
<i>tdm-group-no-2</i>	TDM group number assigned to the second controller.

#### Pass-Through Traffic from a UIO Serial Port to a Trunk Controller

<i>id</i>	Unique ID assigned to this cross connection.
<i>interface-serial</i>	Number of the serial port, either 0 or 1.
<i>controller</i>	Type of the controller. Enter one of the following: T1 0, T1 1, E1 0, or E1 1.
<i>tdm-group-no</i>	TDM group number assigned to the controller.

## customer-id

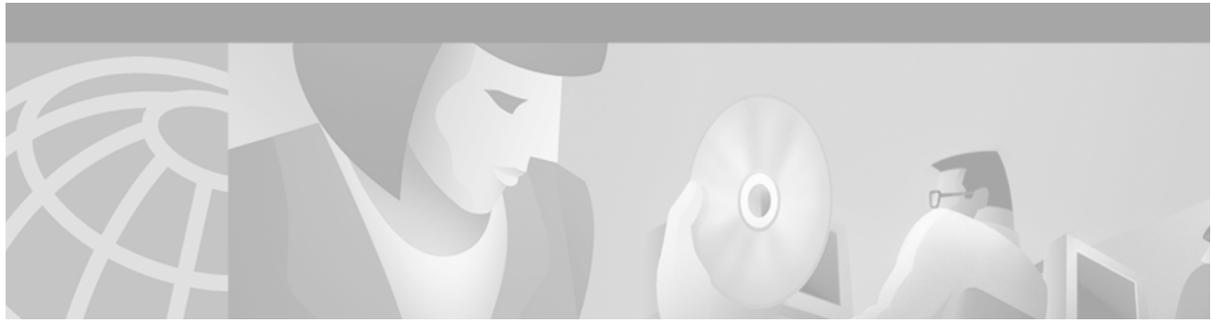
To identify a carrier or Internet service provider (ISP) with a settlement provider, enter the **customer-id** command in settlement configuration mode. To reset the default value of this command, use the **no** form of this command.

**customer-id** *number*

**no customer-id** *number*

<b>Syntax Description</b>	<i>number</i>	Customer ID number as provided by the settlement server. The value range is from 0 to 2,147,483,647.
---------------------------	---------------	--





## Voice, Video, and Fax Commands: default Through ftc-trunk management-protocol

---

This chapter describes the function and syntax of the voice, video, and fax commands from **default** through **ftc-trunk management-protocol**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Voice, Video, and Fax Command Reference*.

### default

To reset the value of a command to its default, use the **default** command in SIP user-agent configuration mode.

```
default {inband-alerting | max-forwards | retry {invite | response | bye | cancel} | sip-server |  
timers {trying | connect | disconnect | expires} | transport}
```

---

#### Syntax Description

<b>inband-alerting</b>	Resets inband-alerting to its default of generating the header “Require: com.cisco.inband-alerting” in outgoing INVITE messages. Tones are fed from the terminating gateway.
<b>max-forwards</b>	Resets max-forwards to its default of 6.
<b>retry {invite   response   bye   cancel}</b>	Resets the specified retry to its default (6 for invite and response; 10 for bye and cancel).
<b>sip-server</b>	Resets the sip-server to a null value.
<b>timers {trying   connect   disconnect   expires}</b>	Resets the specified timer to its default (500 for trying, connect, and disconnect; 180,000 for expires).
<b>transport</b>	Resets transport to the default of both User Datagram Protocol (UDP) and TCP enabled.

---

## default-file vfc

To specify an additional (or different) file from the ones in the default file list and stored in voice feature card (VFC) Flash memory, use the **default-file vfc** command in global configuration mode. To delete the file from the default file list, use the **no** form of this command.

**default-file** *filename vfc slot*

**no default-file** *filename vfc slot*

### Syntax Description

<i>filename</i>	Indicates the file to be retrieved from VFC Flash memory and used (as the default file) to boot up the system.
<i>slot</i>	Indicates the slot on the Cisco AS5300 universal access server in which the VFC is installed. Valid entries are from 0 to 2.

## define

To define the transmit and receive bits for North American ear and mouth (E&M) and E&M Mercury Exchange Limited Channel-Associated Signaling (MELCAS) voice signaling, use the **define** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**define** { *tx-bits* | *rx-bits* } { *seize* | *idle* } { **0000** | **0001** | **0010** | **0011** | **0100** | **0101** | **0110** | **0111** | **1000** | **1001** | **1010** | **1011** | **1100** | **1101** | **1110** | **1111** }

**no define** { *tx-bits* | *rx-bits* } { *seize* | *idle* } { **0000** | **0001** | **0010** | **0011** | **0100** | **0101** | **0110** | **0111** | **1000** | **1001** | **1010** | **1011** | **1100** | **1101** | **1110** | **1111** }

### Syntax Description

<b>tx-bits</b>	The bit pattern applies to the transmit signaling bits.
<b>rx-bits</b>	The bit pattern applies to the receive signaling bits.
<b>seize</b>	The bit pattern defines the seized state.
<b>idle</b>	The bit pattern defines the idle state.
<b>0000</b> through <b>1111</b>	Specifies the bit pattern.

## delete vfc

To delete a file from voice feature card (VFC) Flash memory, use the **delete vfc** command in privileged EXEC mode.

**delete** *filename vfc slot*

### Syntax Description

<i>filename</i>	Specifies the file in VFC Flash memory to be deleted.
<i>slot</i>	Specifies the slot on the Cisco AS5300 universal access server in which the specified VFC resides. Valid entries are from 0 to 2.

## description

To include a specific description about the digital signal processor (DSP) interface, use the **description** command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

**description** *string*

**no description**

---

**Syntax Description***string*Character string from 1 to 80 characters.

---

## description (dspfarm)

To include a specific description about the digital signal processor (DSP) interface, use the **description** command in DSPfarm interface configuration mode. To disable this feature, use the **no** form of this command.

**description** *string*

**no description** *string*

---

**Syntax Description***string*Character string from 1 to 80 characters.

---

## destination-pattern

To specify either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer, use the **destination-pattern** command in dial-peer configuration mode. To disable the configured prefix or telephone number, use the **no** form of this command.

**destination-pattern** [+] *string* [**T**]

**no destination-pattern** [+] *string* [**T**]

<b>Syntax Description</b>	<b>+</b>	(Optional) Character indicating an E.164 standard number.
	<i>string</i>	<p>Series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters:</p> <ul style="list-style-type: none"> <li>The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. On the Cisco 3600 Series routers only, these characters cannot be used as leading characters in a string (for example, *650).</li> <li>Comma (,), which inserts a pause between digits.</li> <li>Period (.), which matches any entered digit (this character is used as a wildcard). On the Cisco 3600 series routers, the period cannot be used as a leading character in a string (for example, .650).</li> <li>Percent sign (%), which indicates that the previous digit/pattern occurred zero or multiple times, similar to the wildcard usage in the regular expression.</li> <li>Plus sign (+), which matches a sequence of one or more matches of the character/pattern.</li> </ul> <p> <b>Note</b> The plus sign used as part of the digit string is different from the plus sign that can be used in front of the digit string to indicate that the string is an E.164 standard number.</p> <ul style="list-style-type: none"> <li>Circumflex (^), which indicates a match to the beginning of the string.</li> <li>Dollar sign (\$), which matches the null string at the end of the input string.</li> <li>Backslash symbol (\), which is followed by a single character matching that character or used with a single character with no other significance (matching that character).</li> <li>Question mark (?), which indicates that the previous digit occurred zero or one time.</li> <li>Brackets ( [ ] ), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. This is similar to a regular expression rule.</li> <li>Parentheses “( )”, which indicate a pattern and is the same as the regular expression rule.</li> </ul>
	<b>T</b>	(Optional) Control character indicating that the <b>destination-pattern</b> value is a variable length dial string.

## destination-pattern (interface)

To specify the ISDN directory number for the telephone interface, use the **destination-pattern** command in interface configuration mode. To disable the specified ISDN directory number, use the **no** form of this command.

**destination-pattern** *isdn*

**no destination-pattern**

<b>Syntax Description</b>	<i>isdn</i>	Local ISDN directory number assigned by your telephone service provider.
---------------------------	-------------	--

## detect v54 channel-group

To enable V.54 loopback detection for the command sent from the remote device, use the **detect v54 channel-group** command in controller configuration mode. To disable the V.54 loopback detection, use the **no** form of this command.

**detect v54 channel-group** *channel-number*

**no detect v54 channel-group** *channel-number*

Syntax Description	<i>channel-number</i>	Channel number from 1 to 24 (T1) or from 1 to 31 (E1).
--------------------	-----------------------	--

## device-id

To identify a gateway associated with a settlement provider, use the **device-id** command in settlement configuration mode. To reset to the default value, use the **no** form of this command.

**device-id** *number*

**no device-id** *number*

Syntax Description	<i>number</i>	Device ID number as provided by the settlement server. Values range is from 0 to 2,147,483,647.
--------------------	---------------	---

## dial-control-mib

To specify attributes for the call history table, use the **dial-control-mib** command in global configuration mode.

**dial-control-mib** {**max-size** *number* | **retain-timer** *number*}

Syntax Description	<b>max-size</b> <i>number</i>	Specifies the maximum size of the call history table. Valid entries are from 0 to 500 table entries. A value of 0 prevents any history from being retained.
	<b>retain-timer</b> <i>number</i>	Specifies the length of time, in minutes, for entries in the call history table. Valid entries are from 0 to 2,147,483,647 minutes. A value of 0 prevents any history from being retained.

## dial-peer hunt

To specify a hunt selection order for dial peers, use the **dial-peer hunt** command in dial-peer configuration mode. To restore the default selection order, use the **no** form of this command.

**dial-peer hunt** *hunt-order-number*

**no dial-peer hunt**

<b>Syntax Description</b>	<i>hunt-order-number</i>	<p>A number from 0 to 7 that selects a predefined hunting selection order:</p> <p>0—Longest match in phone number, explicit preference, random selection. This is the default hunt order number.</p> <p>1—Longest match in phone number, explicit preference, least recent use.</p> <p>2—Explicit preference, longest match in phone number, random selection.</p> <p>3—Explicit preference, longest match in phone number, least recent use.</p> <p>4—Least recent use, longest match in phone number, explicit preference.</p> <p>5—Least recent use, explicit preference, longest match in phone number.</p> <p>6—Random selection.</p> <p>7—Least recent use.</p>
---------------------------	--------------------------	---

## dial-peer terminator

To change the character used as a terminator for variable-length dialed numbers, use the **dial-peer terminator** command in global configuration mode. To restore the default terminating character, use the **no** form of this command.

**dial-peer terminator** *character*

**no dial-peer terminator**

<b>Syntax Description</b>	<i>character</i>	<p>Designates the terminating character for a variable-length dialed number. Valid numbers and characters are #, *, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, and d. The default is #.</p>
---------------------------	------------------	---

## dial-peer video

To define a video ATM dial peer for a local or remote video codec, to specify video-related encapsulation, and to enter dial-peer configuration mode use the **dial-peer video** command in global configuration mode. To remove the video dial peer, use the **no** form of this command.

**dial-peer video** *tag* { **videocodec** | **videoatm** }

**no dial-peer video** *tag* { **videocodec** | **videoatm** }

<b>Syntax Description</b>	<i>tag</i>	Digits that define a particular dial peer. Defines the dial peer and assigns the protocol type to the peer. Valid entries are from 1 to 10,000. The tag must be unique on the router.
	<b>videocodec</b>	Specifies a local video codec connected to the router.
	<b>videoatm</b>	Specifies a remote video codec on the ATM network.

## dial-peer voice

To enter dial-peer configuration mode (and to specify the method of voice encapsulation), use the **dial-peer voice** command in global configuration mode. To disable a defined dial peer, use the **no** form of this command.

### Cisco 2600 Series Routers

```
dial-peer voice tag {pots | vofr | voip}
no dial-peer voice tag {pots | vofr | voip}
```

### Cisco 3600 Series Routers

```
dial-peer voice tag {pots | voatm | vofr | voip}
no dial-peer voice tag
```

### Cisco 7200 Series Routers

```
dial-peer voice tag {vofr}
no dial-peer voice tag {vofr}
```

### Cisco AS5300 universal access server Access Servers

```
dial-peer voice tag {mmoip | pots | vofr | voip}
no dial-peer voice tag {mmoip | pots | vofr | voip}
```

### Cisco MC3810 Multiservice Concentrator

```
dial-peer voice tag {pots | voatm | vofr}
no dial-peer voice tag {pots | voatm | vofr}
```

<b>Syntax Description</b>	<i>tag</i>	Digits that define a particular dial peer. Valid entries are from 1 to 2,147,483,647.
	<b>mmoip</b>	Indicates that this is a multimedia mail peer using IP encapsulation on the IP backbone.
	<b>pots</b>	Indicates that this is a plain old telephone service (POTS) peer using Voice over IP encapsulation on the IP backbone.

<b>voatm</b>	(Cisco 3600 series routers and Cisco MC3810 multiservice concentrators only) Specifies that this is a Voice over ATM dial peer using the real-time AAL5 voice encapsulation on the ATM backbone network.
<b>vofr</b>	Specifies that this is a Voice over Frame Relay dial peer using FRF.11 encapsulation on the Frame Relay backbone network.
<b>voip</b>	Indicates that this is a VoIP peer using voice encapsulation on the POTS network.

## dial-type

To specify the type of out-dialing for voice port interfaces, use the **dial-type** command in voice-port configuration mode. To disable the selected type of dialing, use the **no** form of this command.

**dial-type** { **dtmf** | **pulse** | **mf** }

**no dial-type**

### Syntax Description

<b>dtmf</b>	Dual tone multifrequency (DTMF) touch-tone dialing.
<b>pulse</b>	Pulse (rotary) dialing.
<b>mf</b>	Multifrequency tone dialing.

## digit-strip

To enable digit stripping on a plain old telephone service (POTS) dial-peer call leg, use the **digit-strip** command in dial-peer configuration mode. To disable digit stripping on the dial-peer call leg, use the **no** form of this command.

**digit-strip**

**no digit-strip**

### Syntax Description

This command has no arguments or keywords.

## direct-inward-dial

To enable the direct inward dial (DID) call treatment for the incoming called number, use the **direct-inward-dial** command in dial-peer configuration mode. To disable DID, use the **no** form of this command.

**direct-inward-dial**

**no direct-inward-dial**

### Syntax Description

This command has no arguments or keywords.

## disc\_pi\_off

To enable an H.323 gateway to disconnect a call when it receives a Disconnect message with a progress indicator (PI) value, use the **disc\_pi\_off** command in voice-port configuration mode. To restore the default state, use the **no** form of this command.

**disc\_pi\_off**

**no disc\_pi\_off**

---

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

## disconnect-ack

To configure a Foreign Exchange Station (FXS) voice port to return an acknowledgment upon receipt of a disconnect signal, use the **disconnect-ack** command in voice-port configuration mode. To disable the acknowledgment, use the **no** form of this command.

**disconnect-ack**

**no disconnect-ack**

---

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

## ds0 busyout

To force a DS0 time slot on a controller into the busyout state, use the **ds0 busyout** command in controller configuration mode. To remove the DS0 time slot from the busyout state, use the **no** form of this command.

**ds0 busyout** *ds0-time-slot*

**no ds0 busyout** *ds0-time-slot*

---

**Syntax Description** *ds0-time-slot* DS0 time slots to be forced into the busyout state. The range is from 1 to 24 and can include any combination of time slots.

---

# ds0-group

To specify the DS0 time slots that make up a logical voice port on a T1 or E1 controller and to specify the signaling type by which the router communicates with the PBX or Public Switched Telephone Network (PSTN), use the **ds0-group** command in controller configuration mode. To remove the group and signaling setting, use the **no** form of this command.

## Cisco 2600 and 3600 Series and Cisco MC3810 Multiservice Concentrator—T1

```
ds0-group ds0-group-no timeslots timeslot-list type {e&m-delay-dial | e&m-fgd |
e&m-immediate-start | e&m-wink-start | ext-sig | fgd-eana | fxo-ground-start |
fxo-loop-start | fxs-ground-start | fxs-loop-start}
```

```
no ds0-group ds0-group-no
```

## Cisco 2600 and 3600 Series and Cisco MC3810 Multiservice Concentrator—E1

```
ds0-group ds0-group-no timeslots timeslot-list type {e&m-delay-dial | e&m-immediate-start |
e&m-melcas-delay | e&m-melcas-immed | e&m-melcas-wink | e&m-wink-start | ext-sig |
fgd-eana | fxo-ground-start | fxo-loop-start | fxo-melcas | fxs-ground-start | fxs-loop-start
| fxs-melcas | r2-analog | r2-digital | r2-pulse}
```

```
no ds0-group ds0-group-no
```

## Cisco 7200 and 7500 Series T1 and E1 Voice Ports

```
ds0-group ds0-group-no timeslots timeslot-list type {e&m-delay-dial | e&m-fgd |
e&m-immediate-start | e&m-wink-start | fxs-ground-start | fxs-loop-start |
fxo-ground-start | fxo-loop-start}
```

```
no ds0-group ds0-group-no
```

## Cisco AS5300 universal access server—T1

```
ds0-group ds0-group-no timeslots timeslot-list [service service-type] [type {e&m-fgb | e&m-fgd
| e&m-immediate-start | fxs-ground-start | fxs-loop-start | fgd-eana | fgd-os | r1-itu |
sas-ground-start | sas-loop-start | none}] [tone type] [addr info]
```

```
no ds0-group ds0-group-no
```

## Cisco AS5300 universal access server—E1

```
ds0-group ds0-group-no timeslots timeslot-list type {none | p7 | r2-analog | r2-digital |
r2-lsv181-digital | r2-pulse}
```

```
no ds0-group ds0-group-no
```

## Cisco AS5800 Universal Access Server—T1

```
ds0-group ds0-group-no timeslots timeslot-list type {e&m-fgb | e&m-fgd |
e&m-immediate-start | fxs-ground-start | fxs-loop-start | fgd-eana | r1-itu | r1-modified |
r1-turkey | sas-ground-start | sas-loop-start | none}
```

```
no ds0-group ds0-group-no
```

## Cisco AS5800 E1 Voice Ports

```
ds0-group ds0-group-no timeslots timeslot-list type { e&m-fgb | e&m-fgd |
e&m-immediate-start | fxs-ground-start | fxs-loop-start | p7 | r2-analog | r2-digital |
r2-pulse | sas-ground-start | sas-loop-start | none }
```

```
no ds0-group ds0-group-no
```

## Syntax Description

## For the Cisco 2600 and 3600 Series Routers and Cisco MC3810 Multiservice Concentrators—T1

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
<b>timeslots</b> <i>timeslot-list</i>	Time slot <i>timeslot-list</i> is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows: <ul style="list-style-type: none"> <li>• 2</li> <li>• 1-15,17-24</li> <li>• 1-23</li> <li>• 2,4,6-12</li> </ul>
<b>type</b>	The signaling method selection for the <b>type</b> keyword depends on the connection that you are making. The ear and mouth (E&M) interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The Foreign Exchange Station (FXS) interface allows connection of basic telephone equipment and PBX. The Foreign Exchange Office (FXO) interface is for connecting the central office (CO) to a standard PBX interface where permitted by local regulations; it is often used for off-premise extensions (OPXs). Types are the following: <ul style="list-style-type: none"> <li>• <b>e&amp;m-delay-dial</b>—The originating endpoint sends an off-hook signal and then waits for an off-hook signal followed by an on-hook signal from the destination.</li> <li>• <b>e&amp;m-fgd</b>—E&amp;M Type II Feature Group D.</li> <li>• <b>e&amp;m-immediate-start</b>—E&amp;M immediate start.</li> <li>• <b>e&amp;m-wink-start</b>—E&amp;M Mercury Exchange Limited Channel-Associated Signaling (MELCAS) wink-start signaling support.</li> <li>• <b>ext-sig</b>—An option available only when the <b>mode CCS</b> command is enabled on the Cisco MC3810 multiservice concentrator for FRF.11 transparent common channel signaling (CCS) support.</li> <li>• <b>fgd-cana</b>—Feature Group D exchange access North American.</li> <li>• <b>fxo-ground-start</b>—FXO ground-start signaling support.</li> <li>• <b>fxo-loop-start</b>—FXO loop-start signaling support.</li> <li>• <b>fxs-ground-start</b>—FXS ground-start signaling support.</li> <li>• <b>fxs-loop-start</b>—FXS loop-start signaling support.</li> </ul>

**For the Cisco 2600 and 3600 Series Routers and Cisco MC3810 Multiservice Concentrators—E1**

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
<b>timeslots</b> <i>timeslot-list</i>	<p>Time slot <i>timeslot-list</i> is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows:</p> <ul style="list-style-type: none"> <li>• 2</li> <li>• 1-15,17-24</li> <li>• 1-23</li> <li>• 2,4,6-12</li> </ul>
<b>type</b>	<p>The signaling method selection for the <b>type</b> keyword depends on the connection that you are making. The E&amp;M interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The FXS interface allows connection of basic telephone equipment and PBX. The FXO interface is for connecting the CO to a standard PBX interface where permitted by local regulations; it is often used for OPXs. Types are the following:</p> <ul style="list-style-type: none"> <li>• <b>e&amp;m-delay-dial</b>—The originating endpoint sends an off-hook signal and then waits for an off-hook signal followed by an on-hook signal from the destination.</li> <li>• <b>e&amp;m-immediate-start</b>—E&amp;M immediate start.</li> <li>• <b>e&amp;m-melcas-delay</b>—E&amp;M MELCAS delay-start signaling support.</li> <li>• <b>e&amp;m-melcas-immed</b>—E&amp;M MELCAS immediate-start signaling support.</li> <li>• <b>e&amp;m-melcas-wink</b>—E&amp;M MELCAS wink-start signaling support.</li> <li>• <b>e&amp;m-wink-start</b>—The originating endpoint sends an off-hook signal and waits for a wink start from the destination.</li> <li>• <b>ext-sig</b>—An option available only when the <b>mode CCS</b> command is enabled on the Cisco MC3810 multiservice concentrator for FRF.11 transparent CCS support.</li> <li>• <b>fgd-eana</b>—Feature Group D exchange access North American.</li> <li>• <b>fxo-ground-start</b>—Specifies FXO ground-start signaling.</li> <li>• <b>fxo-loop-start</b>—Specifies FXO loop-start signaling.</li> <li>• <b>fxo-melcas</b>—MELCAS FXO signaling.</li> <li>• <b>fxs-ground-start</b>—FXS ground-start signaling.</li> <li>• <b>fxs-loop-start</b>—FXS loop-start signaling.</li> <li>• <b>fxs-melcas</b>—MELCAS FXS signaling.</li> <li>• <b>r2-analog</b>—Specifies R2 analog line signaling.</li> <li>• <b>r2-digital</b>—Specifies R2 digital line signaling.</li> <li>• <b>r2-pulse</b>—Specifies 7-pulse line signaling, a transmitted pulse that indicates a change in the line state.</li> </ul>

**For the Cisco 7200 and 7500 Series Routers—T1 and E1**

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
<b>timeslots</b> <i>timeslot-list</i>	Time slot <i>timeslot-list</i> is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows: <ul style="list-style-type: none"> <li>• 2</li> <li>• 1-15,17-24</li> <li>• 1-23</li> <li>• 2,4,6-12</li> </ul>
<b>type</b>	The signaling method selection for the <b>type</b> keyword depends on the connection that you are making. The E&M interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The FXS interface allows connection of basic telephone equipment and PBX. The FXO interface is for connecting the CO to a standard PBX interface where permitted by local regulations; it is often used for OPXs. Types are the following: <ul style="list-style-type: none"> <li>• <b>e&amp;m-delay-dial</b>—The originating endpoint sends an off-hook signal and then waits for an off-hook signal followed by an on-hook signal from the destination.</li> <li>• <b>e&amp;m-fgd</b>—E&amp;M Type II Feature Group D.</li> <li>• <b>e&amp;m-immediate-start</b>—E&amp;M immediate start.</li> <li>• <b>e&amp;m-wink-start</b>—E&amp;M MELCAS wink-start signaling support.</li> <li>• <b>fxs-ground-start</b>—FXO ground-start signaling support.</li> <li>• <b>fxs-loop-start</b>—FXS loop start.</li> <li>• <b>fxo-ground-start</b>—Specifies FXO ground-start signaling.</li> <li>• <b>fxo-loop-start</b>—FXO loop-start signaling support.</li> </ul>

**For the Cisco AS5300 Universal Access Server—T1**

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
<b>timeslots</b> <i>timeslot-list</i>	time slot <i>timeslot-list</i> is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows: <ul style="list-style-type: none"> <li>• 2</li> <li>• 1-15,17-24</li> <li>• 1-23</li> <li>• 2,4,6-12</li> </ul>
<b>service</b> <i>service-type</i>	(Optional) Indicates the type of calls to be handled by this DS0 group— <b>data</b> , <b>fax</b> , <b>voice</b> , or <b>mgcp</b> .

<b>type</b>	(Optional) The signaling method selection for the <b>type</b> keyword depends on the connection that you are making. The E&M interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The FXS interface allows connection of basic telephone equipment and PBX. The FXO interface is for connecting the CO to a standard PBX interface where permitted by local regulations; it is often used for OPXs. Types are the following: <ul style="list-style-type: none"> <li>• <b>e&amp;m-fgb</b>—E&amp;M Type II Feature Group B.</li> <li>• <b>e&amp;m-fgd</b>—E&amp;M Type II Feature Group D.</li> <li>• <b>e&amp;m-immediate-start</b>—E&amp;M immediate start.</li> <li>• <b>fxs-ground-start</b>—FXS ground start.</li> <li>• <b>fxs-loop-start</b>—FXS loop start.</li> <li>• <b>fgd-eana</b>—Feature Group D exchange access North American.</li> <li>• <b>fgd-os</b>—Feature Group D operator services.</li> <li>• <b>r1-itu</b>—Line signaling based on international signaling standards.</li> <li>• <b>sas-ground-start</b>—Single attachment station (SAS) ground start.</li> <li>• <b>sas-loop-start</b>—SAS loop start.</li> <li>• <b>none</b>—Null signaling for external call control.</li> </ul>
<b>tone type</b>	(Optional) Specifies the tone as <b>dtmf</b> or <b>mf</b> .
<b>addr info</b>	(Optional) Specifies the calling/called party.

**For the Cisco AS5300 Universal Access Server—E1**

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
<b>timeslots</b> <i>timeslot-list</i>	time slot <i>timeslot-list</i> is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows: <ul style="list-style-type: none"> <li>• 2</li> <li>• 1-15,17-24</li> <li>• 1-23</li> <li>• 2,4,6-12</li> </ul>
<b>type</b>	The signaling method selection for the <b>type</b> keyword depends on the connection that you are making. The E&M interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The FXS interface allows connection of basic telephone equipment and PBX. The FXO interface is for connecting the CO to a standard PBX interface where permitted by local regulations; it is often used for OPXs. Types are the following: <ul style="list-style-type: none"> <li>• <b>none</b>—Null signaling for external call control.</li> <li>• <b>p7</b>—Specifies the p7 switch type.</li> <li>• <b>r2-analog</b>—Specifies R2 analog line signaling.</li> <li>• <b>r2-digital</b>—Specifies R2 digital line signaling.</li> <li>• <b>r2-lsv181-digital</b>—Specifies a specific R2 digital line.</li> <li>• <b>r2-pulse</b>—Specifies 7-pulse line signaling, a transmitted pulse that indicates a change in the line state.</li> </ul>

**For the Cisco AS5300 Universal Access Server—T1**

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
<b>timeslots</b> <i>timeslot-list</i>	<p>time slot <i>timeslot-list</i> is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows:</p> <ul style="list-style-type: none"> <li>• 2</li> <li>• 1-15,17-24</li> <li>• 1-23</li> <li>• 2,4,6-12</li> </ul>
<b>type</b>	<p>The signaling method selection for the <b>type</b> keyword depends on the connection that you are making. The E&amp;M interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The FXS interface allows connection of basic telephone equipment and PBX. The FXO interface is for connecting the CO to a standard PBX interface where permitted by local regulations; it is often used for OPXs. Types are the following:</p> <ul style="list-style-type: none"> <li>• <b>e&amp;m-fgb</b>—E&amp;M Type II Feature Group B.</li> <li>• <b>e&amp;m-fgd</b>—E&amp;M Type II Feature Group D.</li> <li>• <b>e&amp;m-immediate-start</b>—E&amp;M immediate start.</li> <li>• <b>fxs-ground-start</b>—FXS ground start.</li> <li>• <b>fxs-loop-start</b>—FXS loop start.</li> <li>• <b>fgd-eana</b>—Feature Group D exchange access North American.</li> <li>• <b>r1-itu</b>—A line signaling based on international signaling standards.</li> <li>• <b>r1-modified</b>—An international signaling standard that is common to channelized T1/E1 networks.</li> <li>• <b>r1-turkey</b>—A signaling standard used in Turkey.</li> <li>• <b>sas-ground-start</b>—SAS ground start.</li> <li>• <b>sas-loop-start</b>—SAS loop start.</li> <li>• <b>none</b>—Null signaling for external call control.</li> </ul>

**For the Cisco AS5800 Universal Access Server—E1**

<i>ds0-group-no</i>	A value from 0 to 23 that identifies the DS0 group.
<b>timeslots</b> <i>timeslot-list</i>	time slot <i>timeslot-list</i> is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows: <ul style="list-style-type: none"> <li>• 2</li> <li>• 1-15,17-24</li> <li>• 1-23</li> <li>• 2,4,6-12</li> </ul>
<b>type</b>	The signaling method selection for the <b>type</b> keyword depends on the connection that you are making. The E&M interface allows connection for PBX trunk lines (tie lines) and telephone equipment. The FXS interface allows connection of basic telephone equipment and PBX. The FXO interface is for connecting the CO to a standard PBX interface where permitted by local regulations; it is often used for OPXs. Types are the following: <ul style="list-style-type: none"> <li>• <b>e&amp;m-fgb</b>—E&amp;M Type II Feature Group B.</li> <li>• <b>e&amp;m-fgd</b>—E&amp;M Type II Feature Group D.</li> <li>• <b>e&amp;m-immediate-start</b>—E&amp;M immediate start.</li> <li>• <b>fxs-ground-start</b>—FXS ground start.</li> <li>• <b>fxs-loop-start</b>—FXS loop start.</li> <li>• <b>p7</b>—Specifies the p7 switch type.</li> <li>• <b>r2-analog</b>—Specifies R2 analog line signaling.</li> <li>• <b>r2-digital</b>—Specifies R2 digital line signaling.</li> <li>• <b>r2-pulse</b>—Specifies 7-pulse line signaling, a transmitted pulse that indicates a change in the line state.</li> <li>• <b>sas-ground-start</b>—SAS ground start.</li> <li>• <b>sas-loop-start</b>—SAS loop start.</li> <li>• <b>none</b>—Null signaling for external call control.</li> </ul>

**dsn**

To specify that a delivery status notice be delivered to the sender, use the **dsn** command in dial-peer configuration mode. To cancel a specific delay status notice option, use the **no** form of this command.

**dsn** { **delay** | **failure** | **success** }

**no dsn** { **delay** | **failure** | **success** }

Syntax Description		
<b>delay</b>		Indicates that when the mail is sent, the next-hop mailer is requested to send an indication to the FROM address if the mail message is delayed. The definition of delay is made by each mailer and is not controllable by the sender (the Cisco AS5300). Each mailer in the path to the recipient that supports the delivery status notification (DSN) extension receives the same request.
<b>failure</b>		Indicates that when the mail is sent, the next-hop mailer is requested to send a message to the FROM address if the mail message failed to be delivered. Each mailer in the path to the recipient that supports the DSN extension receives the same request.
<b>success</b>		Indicates that when the mail is sent, the next-hop mailer is requested to send a message to the FROM address if the mail message is successfully delivered to the recipient. Each mailer in the path to the recipient that supports the DSN extension receives the same request.

## dspint dspfarm

To enable the digital signal processor (DSP) interface, use the **dspint dspfarm** command in global configuration mode.

```
dspint dspfarm slot/port
```

Syntax Description		
<i>slot</i>		Specifies the slot number of the interface.
<i>port</i>		Specifies the port number of the interface.

## dtmf-relay (Voice over IP)

To specify how an H.323 gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network, use the **dtmf-relay** command in dial-peer configuration mode. To remove all signaling options and to send the DTMF tones as part of the audio stream, use the **no** form of this command.

```
dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal]
```

```
no dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal]
```

Syntax Description		
<b>cisco-rtp</b>		(Optional) Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with a Cisco proprietary payload type.
<b>h245-alphanumeric</b>		(Optional) Forwards DTMF tones by using the H.245 “alphanumeric” User Input Indication method. Supports tones 0-9, *, #, and A-D.
<b>h245-signal</b>		(Optional) Forwards DTMF tones by using the H.245 “signal” User Input Indication method. Supports tones 0-9, *, #, and A-D.

## dtmf-relay (Voice over Frame Relay)

To enable the generation of FRF.11 Annex A frames for a dial peer, use the **dtmf-relay** command in dial-peer configuration mode. To disable the generation of FRF.11 Annex A frames and return to the default handling of dial digits, use the **no** form of this command.

**dtmf-relay**

**no dtmf-relay**

---

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

## dtmf-timer-inter-digit

To configure the dual tone multifrequency (DTMF) interdigit timer for a DS0 group, use the **dtmf-timer-inter-digit** command in T1 controller configuration mode. To restore the timer to its default value, use the **no** form of this command.

**dtmf-timer-inter-digit** *milliseconds*

**no dtmf-timer-inter-digit** *milliseconds*

---

**Syntax Description** *milliseconds* DTMF interdigit timer duration, in milliseconds. The valid range is from 250 to 3000. The default is 3000 milliseconds.

---

## echo-cancel comfort-noise

To specify that background noise be generated, use the **echo-cancel comfort-noise** command in controller configuration mode. To disable this feature, use the **no** form of this command.

**echo-cancel comfort-noise**

**no echo-cancel comfort-noise**

---

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

## echo-cancel compensation

To set attenuation for loud signals, use the **echo-cancel compensation** command in controller configuration. To disable this feature, use the **no** form of this command.

**echo-cancel compensation**

**no echo-cancel compensation**

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

## echo-cancel coverage

To adjust the maximum duration to cancel the voice echo, use the **echo-cancel coverage** command in voice-port configuration mode. To reset this command to the default value, use the **no** form of this command.

**echo-cancel coverage {8 | 16 | 24 | 32}**

**no echo-cancel coverage**

<b>Syntax Description</b>		
<b>8</b>		8 milliseconds.
<b>16</b>		16 milliseconds.
<b>24</b>		24 milliseconds.
<b>32</b>		24 milliseconds.

## echo-cancel enable

To enable the cancellation of voice that is sent out the interface and is received back on the same interface, use the **echo-cancel enable** command in voice-port configuration mode. To disable echo cancellation, use the **no** form of this command.

**echo-cancel enable**

**no echo-cancel enable**

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

## echo-cancel enable (controller)

To enable the echo cancel feature, use the **echo-cancel enable** command in controller configuration mode. To disable this feature, use the **no** form of this command.

**echo-cancel enable**

**no echo-cancel enable**

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

## echo-cancel loopback

To place the echo cancellation processor in loopback mode, use the **echo-cancel loopback** command in controller configuration mode. To disable loopback of the echo cancellation processor, use the **no** form of this command.

**echo-cancel loopback**

**no echo-cancel loopback**

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

## encapsulation

To configure the ATM adaptation layer (AAL) and encapsulation type for Voice over ATM (VoATM), use the **encapsulation** command in interface-ATM-virtual-circuit mode. To remove an encapsulation from a permanent virtual circuit (PVC) class, use the **no** form of this command.

**encapsulation { aal-encap | aal5mux voice | aal5snap | aal2 }**

**no encapsulation**



**Note**

This command reference page describes only AAL2 and encapsulation settings for VoATM. For the full syntax of the **encapsulation** command, refer to *Cisco IOS Wide-Area Networking Command Reference*.

**Syntax Description**

<b>aal-encap</b>	Specifies the AAL and encapsulation type.
<b>aal5mux voice</b>	Specifies a MUX virtual circuit for Voice over ATM.

<b>aal-encap</b>	Specifies the AAL and encapsulation type.
<b>aal5snap</b>	Specifies the only encapsulation supported for Inverse Address Resolution Protocol (ARP). Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram.
<b>aal2</b>	Sets PVC encapsulation to support AAL2 voice traffic on the Cisco MC3810 multiservice concentrator.

## encapsulation atm-ces

To enable circuit emulation service (CES) ATM encapsulation on the Cisco MC3810 multiservice concentrator, use the **encapsulation atm-ces** command in interface configuration mode. To disable CES ATM encapsulation, use the **no** form of this command.

**encapsulation atm-ces**

**no encapsulation atm-ces**

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

## encapsulation ftc-trunk

This command was removed in Cisco IOS Release 12.1(2)T and is no longer supported in this release.

## encryption

To set the algorithm to be negotiated with the provider, use the **encryption** command in settlement configuration mode. To reset to the default encryption method, use the **no** form of this command.

**encryption** { **des-cbc-sha** | **des40-cbc-sha** | **dh-des-cbc-sha** | **dh-des40-cbc-sha** | **null-md5** | **null-sha** | **all** }

**no encryption** { **des-cbc-sha** | **des40-cbc-sha** | **dh-des-cbc-sha** | **dh-des40-cbc-sha** | **null-md5** | **null-sha** | **all** }

<b>Syntax Description</b>	<b>des-cbc-sha</b>	Encryption type ssl_rsa_with_des_cbc_sha cipher suite.
	<b>des40-cbc-sha</b>	Encryption type ssl_rsa_export_with_des40_cbc_sha cipher suite.
	<b>dh-des-cbc-sha</b>	Encryption type ssl_dh_rsa_with_des_cbc_sha cipher suite.
	<b>dh-des40-cbc-sha</b>	Encryption type ssl_dh_rsa_export_with_des40_cbc_sha cipher suite.
	<b>null-md5</b>	Encryption type ssl_rsa_with_null_md5 cipher suite.
	<b>null-sha</b>	Encryption type ssl_rsa_with_null_sha cipher suite.
	<b>all</b>	All encryption methods are used in the Secure Socket Layer (SSL).

## erase vfc

To erase the Flash memory of a specified voice feature card (VFC), use the **erase vfc** command in privileged EXEC mode.

**erase vfc** *slot*

<b>Syntax Description</b>	<i>slot</i>	Specifies the slot on the Cisco AS5300 universal access server in which the specified VFC resides. Valid entries are from 0 to 2.
---------------------------	-------------	---

## expect-factor

To specify when the router generates an alarm to the network manager, indicating that the expected quality of voice has dropped, use the **expect-factor** command in dial-peer configuration mode. To reset the default value, use the **no** form of this command.

**expect-factor** *value*

**no expect-factor** *value*

<b>Syntax Description</b>	<i>value</i>	Integers that represent the International Telecommunication Union (ITU) specification for quality of voice as described in G.113. Valid entries are from 0 to 20, with 0 representing toll quality.
---------------------------	--------------	---

## fax protocol (dial-peer)

To specify the fax protocol for a specific Voice over IP (VoIP) dial peer, use the **fax protocol** command in dial-peer configuration mode. To return to the default fax protocol, use the **fax protocol system** command. To disable the T.38 fax protocol for a specific dial peer, use the **no** form of this command.

**fax protocol** { **cisco** | **t38** [*ls\_redundancy value*] [*hs\_redundancy value*] | **system** }

**no fax protocol**

<b>Syntax Description</b>	<b>cisco</b>	Cisco proprietary fax protocol.
	<b>t38</b>	ITU-T T.38 standard fax protocol.
	<b>ls_redundancy value</b>	(Optional) Low-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 5. The default is 0. The <b>ls_redundancy</b> parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol.

<b>hs_redundancy</b> <i>value</i>	(Optional) High-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 2. The default is 0. The <b>hs_redundancy</b> parameter refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data.
<b>system</b>	Global fax protocol when neither <b>cisco</b> nor <b>t38</b> is specified. The value is taken from the global configuration by default.

## fax protocol (voice-service)

To specify the global default fax protocol for all Voice over IP (VoIP) dial peers, use the **fax protocol** command in voice-service configuration mode. To return to the default fax protocol, use the **no** form of this command.

```
fax protocol { cisco | t38 [ls_redundancy value] [hs_redundancy value]
```

```
no fax protocol
```

Syntax Description	
<b>cisco</b>	Cisco proprietary fax protocol.
<b>t38</b>	ITU-T T.38 standard fax protocol.
<b>ls_redundancy</b> <i>value</i>	(Optional) Low-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 5. The default is 0. The <b>ls_redundancy</b> parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol.
<b>hs_redundancy</b> <i>value</i>	(Optional) High-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 2. The default is 0. The <b>hs_redundancy</b> parameter refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data.

## fax rate

To establish the rate at which a fax is sent to the specified dial peer, use the **fax rate** command in dial-peer configuration mode. To reset the dial peer for voice calls, use the **no** form of this command.

```
fax rate { 2400 | 4800 | 7200 | 9600 | 12000 | 14400 } { disable | voice } [bytes bytes]
```

```
no fax rate
```

Syntax Description	
<b>2400</b>	Specifies a fax transmission speed of 2400 bits per second (bps).
<b>4800</b>	Specifies a fax transmission speed of 4800 bps.
<b>7200</b>	Specifies a fax transmission speed of 7200 bps.
<b>9600</b>	Specifies a fax transmission speed of 9600 bps.
<b>12000</b>	Specifies a fax transmission speed of 12,000 bps.
<b>14400</b>	Specifies a fax transmission speed of 14,400 bps.
<b>disable</b>	Disables Fax Relay transmission capability.

<b>voice</b>	Specifies the highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission may occur up to 14,400 bps because 14,400 bps is less than the 64K voice rate. If the voice codec is G.729 (8K), the fax transmission speed will be 7200 bps.
<b>bytes</b> <i>bytes</i>	(Optional) Selects the fax payload size, in bytes.

## fax receive called-subscriber

To define the called subscriber identifier (CSI), use the **fax receive called-subscriber** command in global configuration mode. To disable the configured number, use the **no** form of this command.

**fax receive called-subscriber** {*\$d\$* | *string*}

**no fax receive called-subscriber** {*\$d\$* | *string*}

<b>Syntax Description</b>	<b>\$d\$</b>	Wildcard that specifies that the information displayed is captured from the configured destination pattern.
	<i>string</i>	Destination telephone number. Valid entries are the plus sign (+), numbers 0 through 9, and the space character. This string can specify an E.164 telephone number; if you choose to configure an E.164 telephone number, use the plus sign as the first character.

## fax-relay ecm disable

To disable fax-relay Error Correction Mode (ECM) on the Voice over IP (VoIP) dial peer, use the **fax-relay ecm disable** command in dial-peer configuration mode. To enable ECM, use the **no** form of this command.

**fax-relay ecm disable**

**no fax-relay ecm disable**

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

## fax send center-header

To specify the data that will appear in the center position of the fax header information, use the **fax send center-header** command in global configuration mode. To disable the selected options, use the **no** form of this command.

**fax send center-header** {*\$a\$* | *\$d\$* | *\$p\$* | *\$s\$* | *\$t\$* | *string*}

**no fax send center-header** {*\$a\$* | *\$d\$* | *\$p\$* | *\$s\$* | *\$t\$* | *string*}

Syntax Description		
	\$a\$	Wildcard that inserts the date in the selected position.
	\$d\$	Wildcard that inserts the destination address in the selected position.
	\$p\$	Wildcard that inserts the page count in the selected position.
	\$s\$	Wildcard that inserts the sender address in the selected position.
	\$t\$	Wildcard that inserts the transmission time in the selected position.
	<i>string</i>	Text string that provides personalized information. Valid characters are any text plus wildcards—for example, Time:\$t\$.

## fax send coverpage comment

To define personalized text for the title field of a fax cover sheet, use the **fax send coverpage comment** command in global configuration mode. To disable the defined comment, use the **no** form of this command.

**fax send coverpage comment** *string*

**no fax send coverpage comment** *string*

Syntax Description		
	<i>string</i>	Text string that adds personalized text in the title field of the fax cover sheet. Valid characters are any ASCII characters.

## fax send coverpage e-mail-controllable

To defer to the cover page setting in the e-mail header to generate a standard fax cover sheet, use the **fax send coverpage e-mail-controllable** command in global configuration mode. To disable standard fax sheet generation, use the **no** form of this command.

**fax send coverpage e-mail-controllable**

**no fax send coverpage e-mail-controllable**

Syntax Description	
	This command has no arguments or keywords.

## fax send coverage enable

To enable the Cisco AS5300 universal access server to generate fax cover sheets for faxes that originate from e-mail messages, use the **fax send coverage enable** command in global configuration mode. To disable the generation of fax cover sheets, use the **no** form of this command.

**fax send coverage enable**

**no fax send coverage enable**

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

## fax send coveragepage show-detail

To print all of the e-mail header information as part of the fax cover sheet, use the **fax send coveragepage show-detail** command in global configuration mode. To disable the e-mail header information being displayed, use the **no** form of this command.

**fax send coveragepage show-detail**

**no fax send coveragepage show-detail**

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

## fax send left-header

To specify the data that will appear on the left in the fax header information, use the **fax send left-header** command in global configuration mode. To disable the selected options, use the **no** form of this command.

**fax send left-header** {**\$a\$** | **\$d\$** | **\$p\$** | **\$s\$** | **\$t\$** | *string*}

**no fax send left-header** {**\$a\$** | **\$d\$** | **\$p\$** | **\$s\$** | **\$t\$** | *string*}

<b>Syntax Description</b>	<b>\$a\$</b>	Wildcard that inserts the date in the selected position.
	<b>\$d\$</b>	Wildcard that inserts the destination address in the selected position.
	<b>\$p\$</b>	Wildcard that inserts the page count in the selected position.
	<b>\$s\$</b>	Wildcard that inserts the sender address in the selected position.
	<b>\$t\$</b>	Wildcard that inserts the transmission time in the selected position.
	<i>string</i>	Text string that provides personalized information. Valid characters are any combination of ASCII characters and the wildcards listed.

## fax send max-speed

To specify the maximum speed at which an outbound fax will be sent, use the **fax send max-speed** command in global configuration mode. To disable the selected speed, use the **no** form of this command.

```
fax send max-speed {2400 | 4800 | 7200 | 9600 | 12000 | 14400}
```

```
no fax send max-speed {2400 | 4800 | 7200 | 9600 | 12000 | 14400}
```

Syntax Description	2400	Indicates a transmission speed of 2400 bits per second (bps).
	4800	Indicates a transmission speed of 4800 bps.
	7200	Indicates a transmission speed of 7200 bps.
	9600	Indicates a transmission speed of 9600 bps.
	12000	Indicates a transmission speed of 12,000 bps.
	14400	Indicates a transmission speed of 14,400 bps.

## fax send right-header

To specify the data that will appear on the right in the fax header information, use the **fax send right-header** command in global configuration mode. To disable the selected options, use the **no** form of this command.

```
fax send right-header {$a$ | $d$ | $p$ | $s$ | $t$ | string}
```

```
no fax send right-header {$a$ | $d$ | $p$ | $s$ | $t$ | string}
```

Syntax Description	\$a\$	Wildcard that inserts the date in the selected position.
	\$d\$	Wildcard that inserts the destination address in the selected position.
	\$p\$	Wildcard that inserts the page count in the selected position.
	\$s\$	Wildcard that inserts the sender address in the selected position.
	\$t\$	Wildcard that inserts the transmission time in the selected position.
	<i>string</i>	Text string that provides personalized information. Valid characters are any combination of ASCII characters and the wildcards listed.

## fax send transmitting-subscriber

To define the transmitting subscriber identifier (TSI), use the **fax send transmitting-subscriber** command in global configuration mode. To disable the configured value, use the **no** form of this command.

```
fax send transmitting-subscriber {$s$ | string}
```

```
no fax send transmitting-subscriber {$s$ | string}
```

<b>Syntax Description</b>	<b>\$s\$</b>	Wildcard that inserts the sender name from the RFC 822 header (captured by the on-ramp from the sending fax machine) in the selected position.
	<i>string</i>	Destination telephone number. Valid entries are the plus sign (+), numbers 0 through 9, and the space character. This string can specify an E.164 telephone number; if you choose to configure an E.164 telephone number, use the plus sign as the first character.

## forward-digits

To specify which digits to forward for voice calls, use the **forward-digits** command in dial-peer configuration mode. To specify that any digits not matching the destination-pattern are not to be forwarded, use the **no** form of this command. To restore the default state, use the **default** form of this command.

**forward-digits** {*num-digit* | **all** | **extra**}

**no forward-digits**

**default forward-digits**

<b>Syntax Description</b>	<i>num-digit</i>	The number of digits to be forwarded. If the number of digits is greater than the length of a destination phone number, the length of the destination number is used. The valid range is from 0 to 32. Setting the value to 0 is equivalent to entering the <b>no forward-digits</b> command.
	<b>all</b>	Forwards all digits. If <b>all</b> is entered, the full length of the destination pattern is used.
	<b>extra</b>	If the length of the dialed digit string is greater than the length of the dial-peer destination pattern, the extra right-justified digits are forwarded. However, if the dial-peer destination pattern is variable length ending with the character "T" (for example: T, 123T, 123...T), extra digits are not forwarded.

## frame-relay voice bandwidth

To specify how much bandwidth should be reserved for voice traffic on a specific data-link connection identifier (DLCI), use the **frame-relay voice bandwidth** command in map-class configuration mode. To release the bandwidth previously reserved for voice traffic, use the **no** form of this command.

**frame-relay voice bandwidth** *bps-reserved* [**queue depth**]

**no frame-relay voice bandwidth** *bps-reserved* [**queue depth**]

<b>Syntax Description</b>	<i>bps-reserved</i>	The bandwidth, in bits per second (bps), reserved for voice traffic for the specified map class. The range is from 8000 to 45,000,000 bps; the default is 0, which disables voice calls.
	<b>queue</b> <i>depth</i>	(Optional) The queue reserved strictly for voice packets. The <i>depth</i> value represents the depth of the queue reserved strictly for voice packets. The default is 100, and the valid range is from 30 to 1000.

## frag-pre-queuing

This command was removed in Cisco IOS Release 12.1(2)T and is no longer supported in this release.

## freq-max-delay

To specify the maximum timing difference allowed between the two frequencies for detection of a tone, use the **freq-max-delay** command in voice-class configuration mode. To restore the default allowed timing difference, use the **no** form of this command.

**freq-max-delay** *time*

**no freq-max-delay**

<b>Syntax Description</b>	<i>time</i>	The maximum number of 10-millisecond time intervals by which the two frequencies in a tone may differ from each other and be detected. The range is from 10 to 100 (100 milliseconds to 1 second). The default is 10 (100 milliseconds).
---------------------------	-------------	--

## freq-max-deviation

To specify the maximum frequency deviation allowed in a tone, use the **freq-max-deviation** command in voice-class configuration mode. To restore the default maximum frequency deviation, use the **no** form of this command.

**freq-max-deviation** *frequency*

**no freq-max-deviation**

<b>Syntax Description</b>	<i>frequency</i>	The maximum cycles per second that the tone frequencies may deviate from the configured frequencies, in Hz, and be detected. The value applies to both frequencies of a dual tone. The range is from 10 to 125. The default is 10.
---------------------------	------------------	--

## freq-max-power

To specify the upper limit of the tone power allowed in a tone, use the **freq-max-power** command in voice-class configuration mode. To restore the default maximum tone power, use the **no** form of this command.

**freq-max-power** *dBmO*

**no freq-max-power**

<b>Syntax Description</b>	<i>dBmO</i>	The upper limit of the tone power that will be detected, in dBmO. The range is from 0 to 20. The default is 10.
---------------------------	-------------	---

## freq-min-power

To specify the lower limit of the tone power allowed in a tone, use the **freq-min-power** command in voice-class configuration mode. To restore the default minimum tone power, use the **no** form of this command.

**freq-min-power** *dBmO*

**no freq-min-power**

<b>Syntax Description</b>	<i>dBmO</i>	The lower limit of the tone power that will be detected, in dBmO. The range is from 10 to 35. The default is 30.
---------------------------	-------------	--

## freq-pair

To specify the frequency components of a tone to be detected, use the **freq-pair** command in voice-class configuration mode. To cancel detection of a tone, use the **no** form of this command.

**freq-pair** *tone-id frequency-1 frequency-2*

**no freq-pair** *tone-id*

<b>Syntax Description</b>	<i>tone-id</i>	A tag identifier for a tone to be detected. The range is from 1 to 16. There is no default.
	<i>frequency-1</i>	One frequency component of the tone to be detected, in Hz. The range is from 300 to 3600. There is no default.
	<i>frequency-2</i>	A second frequency component of the tone to be detected, in Hz. The range is from 300 to 3600, or you can specify 0. There is no default.

## freq-power-twist

To specify the power difference allowed between the two frequencies of a tone, use the **freq-power-twist** command in voice-class configuration mode. To restore the default power difference allowed, use the **no** form of this command.

**freq-power-twist** *dBmO*

**no freq-power-twist**

---

<b>Syntax Description</b>	<i>dBmO</i>	The maximum power difference allowed between the two frequencies of a tone, in dBmO. The range is from 0 to 15. The default is 6.
---------------------------	-------------	---

---

## ftc-trunk frame-relay-dlci

This command was removed in Cisco IOS Release 12.1(2)T and is no longer supported in this release.

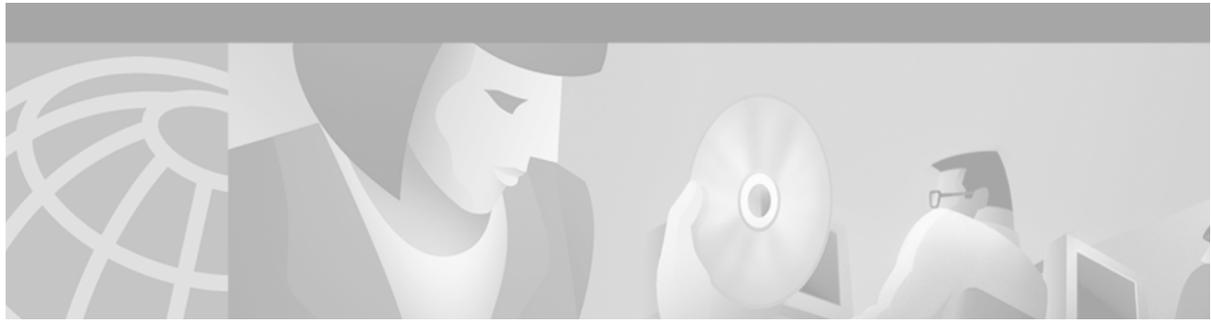
## ftc-trunk management-dlci

This command was removed in Cisco IOS Release 12.1(2)T and is no longer supported in this release.

## ftc-trunk management-protocol

This command was removed in Cisco IOS Release 12.1(2)T and is no longer supported in this release.





## Voice, Video, and Fax Commands: **gatekeeper** Through **proxy h323**

---

This chapter describes the function and syntax of the voice, video, and fax commands from **gatekeeper** through **proxy h323**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Voice, Video, and Fax Command Reference*.

### **gatekeeper**

To enter gatekeeper configuration mode, use the **gatekeeper** command in global configuration mode.

```
gatekeeper
```

---

#### **Syntax Description**

This command has no arguments or keywords.

### **gateway**

To enable the H.323 Voice over IP (VoIP) gateway, use the **gateway** command in global configuration mode. To disable the gateway, use the **no** form of this command.

```
gateway
```

```
no gateway
```

---

#### **Syntax Description**

This command has no arguments or keywords.

## gw-accounting

To enable Voice over IP (VoIP) gateway-specific accounting and define the accounting method, use the **gw-accounting** command in global configuration mode. To disable gateway-specific accounting, use the **no** form of this command.

```
gw-accounting {h323 [vsa] | syslog | voip}
```

```
no gw-accounting {h323 [vsa] | syslog | voip}
```

Syntax Description	h323	Enables standard H.323 accounting using Internet Engineering Task Force (IETF) RADIUS attributes.
	vsa	(Optional) Enables H.323 accounting using RADIUS vendor specific attributes (VSAs).
	syslog	Enables the system logging facility to output accounting information in the form of a system log message.
	voip	Enables generic gateway-specific accounting.

## gw-type-prefix

To configure a technology prefix in the gatekeeper, use the **gw-type-prefix** command in gatekeeper configuration mode. To remove the technology prefix, use the **no** form of this command.

```
gw-type-prefix type-prefix [[hopoff gkid1] [hopoff gkid2] [hopoff gkidn] [seq | blast]]
[default-technology] [[gw ipaddr ipaddr [port]]]
```

```
no gw-type-prefix type-prefix [[hopoff gkid1] [hopoff gkid2] [hopoff gkidn] [seq | blast]]
[default-technology] [[gw ipaddr ipaddr [port]]]
```

Syntax Description	<i>type-prefix</i>	A technology prefix is recognized and is stripped before checking for the zone prefix. It is strongly recommended that you select technology prefixes that do not lead to ambiguity with zone prefixes. Do this by using the # character to terminate technology prefixes, for example, 3#.
	<b>hopoff</b> <i>gkid</i>	(Optional) Use this option to specify the gatekeeper where the call is to hop off, regardless of the zone prefix in the destination address. The <i>gkid</i> argument refers to a gatekeeper previously configured using the zone local or zone remote comment. You can enter this keyword and argument multiple times to configure redundant gatekeepers for a given technology prefix.
	<b>seq   blast</b>	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially or simultaneously (blast) to the gatekeepers according to the order in which they were listed. The default is to send them sequentially.

<b>default-technology</b>	(Optional) Gateways registering with this prefix option are used as the default for routing any addresses that are otherwise unresolved.
<b>gw ipaddr ipaddr [port]</b>	(Optional) Use this option to indicate that the gateway is incapable of registering technology prefixes. When it registers, it adds the gateway to the group for this type prefix, just as if it had sent the technology prefix in its registration. This parameter can be repeated to associate more than one gateway with a technology prefix.

## h225 timeout tcp establish

To set the H.225 TCP timeout value for Voice over IP (VoIP) dial peers, use the **h225 timeout tcp establish** command in voice class configuration mode. To set the timeout value to its default, use the **no** form of this command.

**h225 timeout tcp establish** *seconds*

**no h225 timeout tcp establish**

<b>Syntax Description</b>	<i>seconds</i>	Specifies the number of seconds for the timeout. Possible values are 0 to 30. The default is 15. If you specify 0, the H.225 TCP timer is disabled.
---------------------------	----------------	---

## h323 asr

To enable application-specific routing (ASR) and specify the maximum bandwidth for a proxy, use the **h323 asr** command in interface configuration mode. To remove a bandwidth setting but keep ASR enabled, use **no** form of this command.

**h323 asr** [**bandwidth** *max-bandwidth*]

**no h323 asr** [**bandwidth** *max-bandwidth*]

<b>Syntax Description</b>	<b>bandwidth</b> <i>max-bandwidth</i>	(Optional) Maximum bandwidth on the interface. The value ranges are from 1 to 10,000,000 kbps. If you do not specify the <i>max-bandwidth</i> , the value defaults to the bandwidth on the interface. If you specify <i>max-bandwidth</i> as a value greater than the interface bandwidth, the bandwidth defaults to the interface bandwidth.
---------------------------	--	---

## h323 call start

To force the H.323 Version 2 gateway to use Fast Connect or Slow Connect procedures for all H.323 calls, use the **h323 call start** command in voice-service configuration mode. To restore the default condition, use the **no** form of this command.

**h323 call start** {**fast** | **slow**}

**no h323 call start**

**Syntax Description**

<b>fast</b>	Gateway uses H.323 Version 2 (Fast Connect) procedures.
<b>slow</b>	Gateway uses H.323 Version 1 (Slow Connect) procedures.

## h323 gatekeeper

To specify the gatekeeper associated with a proxy and to control how the gatekeeper is discovered, use the **h323 gatekeeper** command in interface configuration mode. To disassociate the gatekeeper, use the **no** form of this command.

```
h323 gatekeeper [id gatekeeper-id] {ipaddr ipaddr [port] | multicast}
```

```
no h323 gatekeeper [id gatekeeper-id] {ipaddr ipaddr [port] | multicast}
```

**Syntax Description**

<b>id</b> <i>gatekeeper-id</i>	(Optional) The <i>gatekeeper-id</i> argument specifies the gatekeeper name. Typically, this is a Domain Name Server (DNS) name, but it can also be a raw IP address in dotted form. If this parameter is specified, gatekeepers that have either the default or explicit flags set for the subnet of the proxy will respond. If this parameter is not specified, only those gatekeepers with the default subnet flag will respond.
<b>ipaddr</b> <i>ipaddr</i> [ <i>port</i> ]	If this parameter is specified, the gatekeeper discovery message will be unicast to this address and, optionally, the port specified.
<b>multicast</b>	If this parameter is specified, the gatekeeper discovery message will be multicast to the well-known RAS multicast address and port.

## h323-gateway voip bind srcaddr

To designate a source IP address for the voice gateway, use the **h323-gateway voip bind srcaddr** command in interface configuration mode. To remove the source IP address, use the **no** form of the command.

```
h323-gateway voip bind srcaddr ip-address
```

```
no h323-gateway voip bind srcaddr
```

**Syntax Description**

<i>ip-address</i>	Specifies the source IP address in dotted-decimal notation.
-------------------	---

## h323-gateway voip h323-id

To configure the H.323 name of the gateway that identifies this gateway to its associated gatekeeper, use the **h323-gateway voip h323-id** command in interface configuration mode. To disable this defined gateway name, use the **no** form of this command.

```
h323-gateway voip h323-id interface-id
```

```
no h323-gateway voip h323-id interface-id
```

<b>Syntax Description</b>	<i>interface-id</i>	H.323 name (ID) used by this gateway when this gateway communicates with its associated gatekeeper. Usually, this ID is the name of the gateway with the gatekeeper domain name appended to the end: name@domain-name.
---------------------------	---------------------	---

## h323-gateway voip id

To define the name and location of the gatekeeper for a specific gateway, use the **h323-gateway voip id** command in interface configuration mode. To disable this gatekeeper identification, use the **no** form of this command.

```
h323-gateway voip id gatekeeper-id {ipaddr ip-address [port-number] | multicast}
[priority number]
```

```
no h323-gateway voip id gatekeeper-id {ipaddr ip-address [port-number] | multicast}
[priority number]
```

<b>Syntax Description</b>	<i>gatekeeper-id</i>	Indicates the H.323 identification of the gatekeeper. This value must exactly match the gatekeeper ID in the gatekeeper configuration. The recommended format is <i>name.doman-name</i> .
	<b>ipaddr</b>	Indicates that the gateway will use an IP address to locate the gatekeeper.
	<i>ip-address</i>	Defines the IP address used to identify the gatekeeper.
	<i>port-number</i>	(Optional) Defines the port number used.
	<b>multicast</b>	Indicates that the gateway will use multicast to locate the gatekeeper.
	<b>priority number</b>	(Optional) The priority of this gatekeeper. The range is 1 through 127, and the default value is 127.

## h323-gateway voip interface

To configure an interface as an H.323 gateway interface, use the **h323-gateway voip interface** command in interface configuration mode. To disable H.323 gateway functionality for an interface, use the **no** form of this command.

```
h323-gateway voip interface
```

```
no h323-gateway voip interface
```

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

## h323-gateway voip tech-prefix

To define the technology prefix that the gateway will register with the gatekeeper, use the **h323-gateway voip tech-prefix** command in interface configuration mode. To disable this defined technology prefix, use the **no** form of this command.

**h323-gateway voip tech-prefix** *prefix*

**no h323-gateway voip tech-prefix** *prefix*

<b>Syntax Description</b>	<i>prefix</i>	Defines the numbers used as the technology prefixes. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound symbol (#) is frequently used as the last digit in a technology prefix. Valid characters are 0 through 9, the pound symbol (#), and the asterisk (*).
---------------------------	---------------	---

## h323 h323-id

To register an H.323 proxy alias with a gatekeeper, use the **h323 h323-id** command in interface configuration mode. To remove an H.323 proxy alias, use the **no** form of this command.

**h323 h323-id** *h323-id*

**no h323 h323-id** *h323-id*

<b>Syntax Description</b>	<i>h323-id</i>	Specifies the name of the proxy. It is recommended that this name be a fully qualified e-mail ID, with the domain name being the same as that of its gatekeeper.
---------------------------	----------------	--

## h323 interface

To select an interface whose IP address will be used by the proxy to register with the gatekeeper, use the **h323 interface** command in interface configuration mode. To use the default port, use the **no h323 interface** and then the **h323 interface** command.

**h323 interface** [*port-number*]

**no h323 interface** [*port-number*]

<b>Syntax Description</b>	<i>port-number</i>	(Optional) The port number the proxy will listen on for incoming call setup requests. Range is 1 to 65,356. The default port number for the proxy is 11,720 in -isx- or -jsx- Cisco IOS images. The default port number for the proxy is 1720 in -ix- Cisco IOS images, which do not contain the VoIP gateway.
---------------------------	--------------------	--

## h323 qos

To enable quality of service (QoS) on the proxy, use the **h323 qos** command in interface configuration mode. To disable QoS, use the **no** form of this command.

```
h323 qos {ip-precedence value | rsvp {controlled-load | guaranteed-qos}}
```

```
no h323 qos {ip-precedence value | rsvp {controlled-load | guaranteed-qos}}
```

### Syntax Description

<b>ip-precedence</b> <i>value</i>	Specifies that RTP streams should set their IP precedence bits to the specified value.
<b>rsvp controlled-load</b>	Specifies controlled load class of service.
<b>rsvp guaranteed-qos</b>	Specifies guaranteed QoS class of service.

## h323 t120

To enable the T.120 capabilities on your router and to specify bypass or proxy mode, use the **h323 t120** command in interface configuration mode.

```
h323 t120 {bypass | proxy}
```

### Syntax Description

<b>bypass</b>	Bypass mode. In this mode, the H.245 Open Logical Channel messages for T.120 data channels are passed unmodified through the proxy, and TCP connections for T.120 are established directly between the two endpoints of the H.323 call.
<b>proxy</b>	Proxy mode. In this mode, T.120 features function properly.

## huntstop

To disable all dial-peer hunting if a call fails when using hunt groups, use the **huntstop** command in dial-peer configuration mode. To reenable dial-peer hunting, use the **no** form of this command.

```
huntstop
```

```
no huntstop
```

### Syntax Description

This command has no arguments or keywords.

## icpif

To specify the Impairment/Calculated Planning Impairment Factor (ICPIF) for calls sent by a dial peer, use the **icpif** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

**icpif** *integer*

**no icpif** *integer*

Syntax Description	<i>integer</i>	Integer, expressed in equipment impairment factor units, that specifies the ICPIF value. Valid entries are 0 to 55. The default is 30.
--------------------	----------------	--

## idle-voltage

To specify the idle voltage on an Foreign Exchange Station (FXS) voice port, use the **idle-voltage** command in voice-port configuration mode. To restore the default idle voltage, use the **no** form of this command.

**idle-voltage** {**high** | **low**}

**no idle-voltage**

Syntax Description	<b>high</b>	The talk-battery (tip-to-ring) voltage is high (–48V) when the FXS port is idle.
	<b>low</b>	The talk-battery (tip-to-ring) voltage is low (–24V) when the FXS port is idle.

## ignore

To configure the North American E&M or E&M MELCAS voice port to ignore specific receive bits, use the **ignore** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**ignore** {**rx-a-bit** | **rx-b-bit** | **rx-c-bit** | **rx-d-bit**}

**no ignore** {**rx-a-bit** | **rx-b-bit** | **rx-c-bit** | **rx-d-bit**}

Syntax Description	<b>rx-a-bit</b>	Ignores the receive A bit.
	<b>rx-b-bit</b>	Ignores the receive B bit.
	<b>rx-c-bit</b>	Ignores the receive C bit.
	<b>rx-d-bit</b>	Ignores the receive D bit.

## image encoding

To select a specific encoding method for fax images associated with an MMoIP dial peer, use the **image encoding** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

**image encoding** { **mh** | **mr** | **mmr** | **passthrough** }

**no image encoding** { **mh** | **mr** | **mmr** | **passthrough** }

Syntax Description	Command	Description
	<b>mh</b>	Specifies Modified Huffman image encoding. This is the IETF standard.
	<b>mr</b>	Specifies Modified Read image encoding.
	<b>mmr</b>	Specifies Modified Modified Read image encoding.
	<b>passthrough</b>	Specifies that the image will not be modified by an encoding method.

## image resolution

To specify a particular fax image resolution for a specific MMoIP dial peer, use the **image resolution** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

**image resolution** { **fine** | **standard** | **superfine** | **passthrough** }

**no image resolution** { **fine** | **standard** | **superfine** | **passthrough** }

Syntax Description	Command	Description
	<b>fine</b>	Configures the fax TIFF image resolution to be 204-by-196 pixels per inch.
	<b>standard</b>	Configures the fax TIFF image resolution to be 204-by-98 pixels per inch.
	<b>superfine</b>	Configures the fax TIFF image resolution to be 204-by-391 pixels per inch.
	<b>passthrough</b>	Indicates that the resolution of the fax TIFF image will not be altered.

## impedance

To specify the terminating impedance of a voice-port interface, use the **impedance** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**impedance** { **600c** | **600r** | **900c** | **complex1** | **complex2** }

**no impedance** { **600c** | **600r** | **900c** | **complex1** | **complex2** }

Syntax Description	Command	Description
	<b>600c</b>	Specifies 600 ohms (complex).
	<b>600r</b>	Specifies 600 ohms (real).
	<b>900c</b>	Specifies 900 ohms (complex).
	<b>complex1</b>	Specifies complex 1.
	<b>complex2</b>	Specifies complex 2.

## incoming called-number

To specify an incoming called number of an Mail Message over IP (MMoIP) or plain old telephone service (POTS) dial peer, use the **incoming called-number** command in dial-peer configuration mode. To reset the default value, use the **no** form of this command.

**incoming called-number** *string*

**no incoming called-number** *string*

<b>Syntax Description</b>	<i>string</i>	Specifies the incoming called telephone number. Valid entries are any series of digits that specify the E.164 telephone number.
---------------------------	---------------	---

## information-type

To select a particular information type for either an Mail Message over IP (MMoIP) or Plain Old Telephone Service (POTS dial peer, use the **information-type** command in dial-peer configuration mode. To reset the default value for this command, use the **no** form of this command.

**information-type** {**fax** | **voice**}

**no information-type** {**fax** | **voice**}

<b>Syntax Description</b>	<b>fax</b>	Indicates that the information type has been set to store and forward fax.
	<b>voice</b>	Indicates that the information type has been set to voice.

## input gain

To configure a specific input gain value, use the **input gain** command in voice-port configuration mode. To disable the selected amount of inserted gain, use the **no** form of this command.

**input gain** *decibels*

**no input gain** *decibels*

<b>Syntax Description</b>	<i>decibels</i>	Specifies, in decibels, the amount of gain to be inserted at the receiver side of the interface. Acceptable values are integers from -6 to 14.
---------------------------	-----------------	--

## ip precedence (dial-peer)

To set IP precedence (priority) for packets sent by the dial peer, use the **ip precedence** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

**ip precedence** *number*

**no ip precedence** *number*

---

**Syntax Description**

*number* Integer specifying the IP precedence value. Valid entries are from 0 to 7. A value of 0 means that no precedence (priority) has been set.

---

## ip udp checksum

To calculate the UDP checksum for voice packets sent by the dial peer, use the **ip udp checksum** command in dial-peer configuration mode. To disable this feature, use the **no** form of this command.

**ip udp checksum**

**no ip udp checksum**

---

**Syntax Description**

This command has no arguments or keywords.

## isdn contiguous-bchan

To configure contiguous bearer channel handling on an E1 PRI interface, use the **isdn contiguous-bchan** command in interface configuration mode. To disable the contiguous B-channel handling, use the **no** form of this command.

**isdn contiguous-bchan**

**no isdn contiguous-bchan**

---

**Syntax Description**

This command has no arguments or keywords.

## isdn global-disconnect

To allow passage of “release” and “release complete” messages over the voice network, use the **isdn global-disconnect** command in interface configuration mode. To disable the passage of these messages, use the **no** form of this command.

**isdn global-disconnect**

**no isdn global-disconnect**

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

## isdn i-number

To configure several terminal devices to use one subscriber line, use the **isdn i-number** command in interface configuration mode.

**isdn i-number** *n ldn*

Syntax Description	<i>n</i>	Subscriber line 1, 2, or 3, as specified in the NTT specification.
	<i>ldn</i>	LDN assigned to the router POTS port.

## isdn network-failure-cause

To specify the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures, use the **isdn network-failure-cause** command in interface configuration mode. To unconfigure the use of this cause code, use the **no** form of this command.

**isdn network-failure-cause** *value*

**no isdn network-failure-cause** *value*

Syntax Description	<i>value</i>	Number from 1 to 127. See Table 9 for a list of failure cause code values.
--------------------	--------------	--

**Table 9 ISDN Failure Cause Codes**

Failure Cause Code	Meaning
1	Unallocated or unassigned number
2	No route to specified transit network
3	No route to destination
6	Channel unacceptable.
7	Call awarded and being delivered in an established channel.

**Table 9 ISDN Failure Cause Codes (continued)**

<b>Failure Cause Code</b>	<b>Meaning</b>
16	Normal call clearing.
17	User busy.
18	No user responding.
19	No answer from user (user alerted).
21	Call rejected.
22	Number changed.
26	Nonselected user clearing.
27	Destination out of order.
28	Invalid number format.
29	Facility rejected.
30	Response to status enquiry.
31	Normal, unspecified.
34	No circuit/channel available.
38	Network out of order.
41	Temporary failure.
42	Switch congestion.
43	Access information discarded.
44	Requested channel not available.
45	Preempted.
47	Resources unavailable, unspecified.
49	Quality of service unavailable.
50	Requested facility not subscribed.
52	Outgoing calls barred.
54	Incoming calls barred.
57	Bearer capability not authorized.
58	Bearer capability not available now.
63	Service or option not available, unspecified.
65	Bearer capability not implemented.
66	Channel type not implemented.
69	Requested facility not implemented.
70	Only restricted digital information bearer capability is available.
79	Service or option not implemented, unspecified.
81	Invalid call reference value.
82	Identified channel does not exist.
83	Suspended call exists, but this call ID does not.
84	Call ID in use.

**Table 9** ISDN Failure Cause Codes (continued)

Failure Cause Code	Meaning
85	No call suspended.
86	Call with requested call ID is cleared.
88	Incompatible destination.
91	Invalid transit network selection.
95	Invalid message, unspecified.
96	Mandatory information element missing.
97	Message type nonexistent or not implemented.
98	Message not compatible with call state or message type nonexistent or not implemented.
99	Information element nonexistent or not implemented.
100	Invalid information element contents.
101	Message not compatible with call state.
102	Recovery on timer expiry.
111	Protocol error, unspecified.
127	Interworking, unspecified.

## ivr autoloading

To load files from a particular TFTP server (as indicated by a defined URL), use the **ivr autoloading** command in global configuration mode. To disable this function, use the **no** form of this command.

**ivr autoloading** *url location*

**no ivr autoloading** *url location*

Syntax Description		
<b>url</b>	Indicates that a URL is used to locate the index file that contains a list of all available audio files.	
<i>location</i>	Specifies the URL of the index file.	

## ivr autoloading retry

To specify the number of times that the system will try to load audio files from TFTP to memory when there is an error, use the **ivr autoloading retry** command in global configuration mode. To disable this function, use the **no** form of this command.

**ivr autoloading retry** *number*

**no ivr autoloading retry** *number*

Syntax Description	<i>number</i>	Number from 1 to 5. The default value is 3.

## ivr autoload mode

To load files from TFTP to memory using either verbose or silent mode, use the **ivr autoload mode** command in global configuration mode. To disable this function, use the **no** form of this command.

**ivr autoload mode** { **verbose url** *location* [**retry** *number*] } | { **silent url** *location* [**retry** *number*] }

**no ivr autoload mode** { **verbose url** *location* [**retry** *number*] } | { **silent url** *location* [**retry** *number*] }

Syntax Description		
<b>verbose</b>		Displays the file transfer activity to the console. This mode is recommended while debugging.
<b>silent</b>		Performs the file transfer in silent mode, meaning that no file transfer activity is displayed to the console.
<b>retry</b>		(Optional) Specifies the number of times the system will try to transfer a file when there are errors. This parameter applies to each file transfer.
<i>number</i>		(Optional) Number of times from 1 to 5. The default value is 3.
<b>url</b>		Indicates that a URL is used to locate the index file that contains a list of all available audio files.
<i>location</i>		Specifies the URL of the index file.

## ivr prompt memory

To configure the maximum amount of memory that the dynamic audio files (prompts) occupy in memory, use the **ivr prompt memory** command in global configuration mode. To disable the maximum memory size, use the **no** form of this command.

**ivr prompt memory** *size files number*

**no ivr prompt memory** *size files number*

Syntax Description		
<i>size</i>		Specifies the maximum memory to be used by the free dynamic prompts, in kilobytes. Valid entries are from 128 to 16,384.
<b>files</b> <i>number</i>		Specifies the number of files that can stay in memory. Valid entries for the number argument are 50 to 1000.

## line-power

To configure the BRI port to supply line power to the terminal equipment (TE), use the **line-power** command in interface configuration mode. 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.

## loopback

To set the loopback method for testing the T1 interface, use the **loopback** command in controller configuration mode. To restore the default value, use the **no** form of this command.

**loopback** { **diagnostic** | **local** { **payload** | **line** } | **remote** { **v54 channel-group** *channel-number* | **iboc** | **esf** { **payload** | **line** } }

**no loopback**

### Syntax Description

<b>diagnostic</b>	Loops the outgoing transmit signal back to the receive signal.
<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>line</b>	Places the interface into external loopback mode at the line.
<b>remote</b>	Keeps the local end of the connection in remote loopback mode.
<b>v54 channel-group</b>	Activates a V.54 channel-group loopback at the remote end. Available for both T1 and E1 facilities.
<i>channel-number</i>	Specifies the channel number range (from 0 to 1) for the V.54 channel-group loopback.
<b>iboc</b>	Activates the remote line loopback by sending inband CSU code.
<b>esf</b>	Only available under T1 controllers when Extended Super Frame (ESF) is configured on the controller. The following are keywords: <ul style="list-style-type: none"> <li>• <b>payload</b>—Activates remote payload loopback by sending Facility Data Link (FDL) code. FDL is a 4-kbps out-of-band signaling channel in ESF.</li> <li>• <b>line</b>—Activates remote line loopback by sending FDL code.</li> </ul>

## loop-detect

To enable loop detection for T1, use the **loop-detect** command in controller configuration mode. To cancel the loop detect operation, use the **no** form of this command.

**loop-detect**

**no loop-detect**

### Syntax Description

This command has no arguments or keywords.

## loss-plan

To specify the analog-to-digital gain offset for an analog Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) voice port, use the **loss-plan** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**loss-plan {plan1 | plan2 | plan3 | plan4 | plan5 | plan6 | plan7 | plan8 | plan9}**

**no loss-plan**

### Syntax Description

<b>plan1</b>	FXO: A-D gain = 0 dB, D-A gain = 0 dB. FXS: A-D gain = -3 dB, D-A gain = -3 dB.
<b>plan2</b>	FXO: A-D gain = 3 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -3 dB.
<b>plan3</b>	FXO: A-D gain = -3 dB, D-A gain = 0 dB. FXS: Not applicable.
<b>plan4</b>	FXO: A-D gain = -3 dB, D-A gain = -3 dB. FXS: Not applicable.
<b>plan5</b>	FXO: Not applicable. FXS: A-D gain = -3 dB, D-A gain = -10 dB.
<b>plan6</b>	FXO: Not applicable. FXS: A-D gain = 0 dB, D-A gain = -7 dB.
<b>plan7</b>	FXO: A-D gain = 7 dB, D-A gain = 0 dB. FXS: A-D gain = 0 dB, D-A gain = -6 dB.
<b>plan8</b>	FXO: A-D gain = 5 dB, D-A gain = -2 dB. FXS: Not applicable.
<b>plan9</b>	FXO: A-D gain = 6 dB, D-A gain = 0 dB. FXS: Not applicable.

## Irq forward-queries

To enable a gatekeeper to forward Location Requests (LRQs) that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers, use the **irq forward-queries** command in gatekeeper configuration mode. To disable this function, use the **no** form of this command.

**irq forward-queries**

**no irq forward-queries**

---

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

## Irq reject-unknown-prefix

To enable the gatekeeper to reject all Location Requests (LRQs) for zone prefixes that are not configured, use the **irq reject-unknown-prefix** command in gatekeeper configuration mode. To reenble the gatekeeper to accept and process all incoming LRQs, use the **no** form of this command.

**irq reject-unknown-prefix**

**no irq reject-unknown-prefix**

---

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

## Irq timeout blast window

To configure the timeout window for use when sending multiple Location Requests (LRQs) (either sequentially or simultaneously), use the **irq timeout blast window** command in gatekeeper configuration mode. To return to the default value, use the **no** form of this command.

**irq timeout blast window** *seconds*

**no irq timeout blast window**

---

<b>Syntax Description</b>	<i>seconds</i>	The duration of the window, in seconds. Possible values are 1 through 10. The default is 6.
---------------------------	----------------	---

---

## lrq timeout seq delay

To configure the delay for use when sending Location Requests (LRQs) sequentially, use the **lrq timeout seq delay** command in gatekeeper configuration mode. To return to the default value, use this **no** form of the command.

**lrq timeout seq delay** *value*

**no lrq timeout seq delay**

---

**Syntax Description***value*

The duration of the delay, in 100 millisecond units. Possible values are 1 through 10. The default is 5 (500 ms or 0.5 seconds).

---

## max-conn

To specify the maximum number of allowed connections for a particular Voice over IP (VoIP) or POTS dial peer, use the **max-conn** command in dial-peer configuration mode. To set an unlimited number of connections for this dial peer, use the **no** form of this command.

**max-conn** *number*

**no max-conn**

---

**Syntax Description***number*

Specifies the maximum number of connections for this dial peer. Valid values for this field are 1 to 2,147,483,647.

---

## max-connection

To set the maximum number of simultaneous connections to be used for communication with a settlement provider, use the **max-connection** command in settlement configuration mode. To reset to the default value of this command, use the **no** form of this command.

**max-connection** *number*

**no max-connection** *number*

---

**Syntax Description***number*

Specifies the maximum number of HTTP connections to a settlement provider.

---

## max-forwards

To set the maximum number of proxy or redirect servers that can forward the request, use the **max-forwards** command in the SIP user agent configuration mode. To reset the default value, use the **no** form of this command.

**max-forwards** *number*

**no max-forwards**

<b>Syntax Description</b>	<i>number</i>	Number of hops. Possible values are 1 through 15. The default is 6.
---------------------------	---------------	---

## max-redirects

To set the maximum number of redirect servers that the user agent allows, use the **max-redirects** command in dial-peer configuration mode. To reset the default value, use the **no** form of this command.

**max-redirects** *number*

**no max-redirects**

<b>Syntax Description</b>	<i>number</i>	Maximum number of redirect servers that a call can traverse. Possible values are 1 through 10.
---------------------------	---------------	--

## mdn

To request that a message disposition notice (MDN) be generated when the message is processed (“opened”), use the **mdn** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

**mdn**

**no mdn**

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

## mgcp

To allocate resources for the MGCP and start the daemon, use the **mgcp** command in global configuration mode. To terminate all calls, release all allocated resources, and stop the MGCP daemon, use the **no** form of this command.

**mgcp** [*port*]

**no mgcp**

<b>Syntax Description</b>	<i>port</i>	(Optional) Specifies a UDP port for the MGCP gateway. Valid values are 1025 through 65,535. If no port is specified, the command defaults to UDP port 2427.
---------------------------	-------------	---

## mgcp block-newcalls

To block new calls while maintaining existing calls, use the **mgcp block-newcalls** command in global configuration mode. To resume MGCP operation, use the **no** form of this command.

**mgcp block-newcalls**

**no mgcp block-newcalls**

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

## mgcp call-agent

To configure the call agent (media gateway controller) address, use the **mgcp call-agent** command in global configuration mode. To unconfigure the call agent address, use the **no** form of this command.

**mgcp call-agent** {*ip-address* | *host-name*} [*port*] [**service-type** *type*]

**no mgcp call-agent**

<b>Syntax Description</b>	<i>ip-address</i>   <i>host-name</i>	Specifies the IP address or domain name of the call agent.
	<i>port</i>	(Optional) Specifies the UDP port for the call agent to use. Valid values are 1025 through 65,535. If a port is not specified, the default is UDP 2427.
	<b>service-type</b> <i>type</i>	(Optional) Specifies the type of gateway control service to be supported by the call agent. Valid values are <b>mgcp</b> and <b>sgcp</b> .

## mgcp codec

To select the default codec type and its optional packetization period value, use the **mgcp codec** command in global configuration mode. To set the parameters to their default values, use the **no** form of this command.

**mgcp codec** *type* [**packetization-period** *value*]

**no mgcp codec**

<b>Syntax Description</b>	<i>type</i>	Specifies the types of codec supported. Valid codecs are G711alaw, G711ulaw, G723ar53, G723ar63, G723r53, G723r63, G729ar8, G729br8, and G729r8.
	<b>packetization-period</b> <i>value</i>	(Optional) This parameter is useful when the preferred compression algorithm and packetization period parameter is not provided by the Media Gateway Controller. The value range depends on the type of codec selected.  For example, the range for G729r8 is 10 to 220 in increments of 10. For G711ulaw, the range is 10 to 20 in increments of 10. For G723ur53, the range is 30 to 330 in increments of 10.

## mgcp default-package

To configure the default package capability type for the media gateway, use the **mgcp default-package** command in global configuration mode. This command does not support a **no** form. To change the default package, use the **mgcp default-package** command with a different, actively supported package.

### Residential Gateways

```
mgcp default-package {line-package | dtmf-package | gm-package}
```

### Trunking Gateways

```
mgcp default-package {as-package | dtmf-package | gm-package | rtp-package |
trunk-package}
```

<b>Syntax Description</b>	<b>as-package</b>	Announcement server package.
	<b>dtmf-package</b>	DTMF package.
	<b>gm-package</b>	Generic media package.
	<b>line-package</b>	Line package.
	<b>rtp-package</b>	RTP package.
	<b>trunk-package</b>	Trunk package.

## mgcp dtmf-relay

To ensure accurate forwarding of digits on compressed codecs, use the **mgcp dtmf-relay** command in controller configuration mode. To disable this process for noncompressed codecs, use the **no** form of this command.

```
mgcp dtmf-relay {codec | low-bit-rate} mode {cisco | out-of-band}
```

```
no mgcp dtmf-relay
```

<b>Syntax Description</b>	<b>codec</b>	Specifies use of either a G.711 or a G.726 codec.
	<b>low-bit-rate</b>	Specifies a low-bit-rate codec other than G.711 and G.726.

<b>mode</b>	Specifies the mode.
<b>cisco</b>	This mode removes the DTMF tone from the voice stream and sends FRF.11 with a special payload 121 for the DTMF digits.
<b>out-of-band</b>	This mode removes the DTMF tone from the voice stream and does not send FRF.11.

## mgcp ip-tos

To enable or disable the IP type of service (ToS) for MGCP-controlled connections, use the **mgcp ip-tos** command in global configuration mode. To set the parameters to their default values, use the **no** form of this command.

```
mgcp ip-tos {high-reliability | high-throughput | low-cost | low-delay | precedence value}
```

```
no mgcp ip-tos {high-reliability | high-throughput | low-cost | low-delay | precedence value}
```

Syntax Description		
<b>high-reliability</b>	Specifies high-reliability ToS.	
<b>high-throughput</b>	Specifies high-throughput ToS.	
<b>low-cost</b>	Specifies low-cost ToS.	
<b>low-delay</b>	Specifies low-delay ToS.	
<b>precedence value</b>	Specifies the value of the IP precedence bit. Valid values are from 0 to 7. The default IP precedence value is 3.	

## mgcp max-waiting-delay

To specify the MGCP maximum waiting delay (MWD), use the **mgcp max-waiting-delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
mgcp max-waiting-delay milliseconds
```

```
no mgcp max-waiting-delay
```

Syntax Description		
<i>milliseconds</i>	The number of milliseconds to wait after restart. The valid range is 0 to 600,000 milliseconds (600 seconds).	

## mgcp modem passthru

To enable the gateway to send and receive modem and fax data, use the **mgcp modem passthru** command in controller configuration mode. To disable support for modem and fax data, use the **no** form of this command.

```
mgcp modem passthru {cisco | ca}
```

```
no mgcp modem passthru
```

<b>Syntax Description</b>	<b>cisco</b>	When the gateway detects a modem/fax tone, the gateway switches the codec to G.711 to allow the analog data to pass through.
	<b>ca</b>	When the gateway detects a modem/fax tone, the gateway alerts the call agent to switch the codec to G.711 to allow the analog data to pass through.

## mgcp package-capability

To specify an MGCP package capability for a gateway, use the **mgcp package-capability** command in global configuration mode. To remove a specific MGCP package capability from the list of capabilities, use the **no** form of this command.

### All Residential Gateways

```
mgcp package-capability {line-package | dtmf-package | gm-package | rtp-package}
```

```
no mgcp package-capability {line-package | dtmf-package | gm-package | rtp-package}
```

### Cisco AS5300 Universal Access Server

```
mgcp package-capability {trunk-package | dtmf-package | gm-package | rtp-package |
as-package | script-package}
```

```
no mgcp package-capability {trunk-package | dtmf-package | gm-package | rtp-package |
as-package | script-package}
```

### All Other Trunking Gateways

```
mgcp package-capability {trunk-package | dtmf-package | gm-package | rtp-package |
as-package}
```

```
no mgcp package-capability {trunk-package | dtmf-package | gm-package | rtp-package |
as-package}
```

<b>Syntax Description</b>	<b>line-package</b>	Line package.
	<b>trunk-package</b>	Trunk package.
	<b>dtmf-package</b>	DTMF package.
	<b>gm-package</b>	Generic media package.
	<b>rtp-package</b>	RTP package.
	<b>as-package</b>	Announcement server package.
	<b>script-package</b>	Script package.

## mgcp playout

To tune the jitter buffer packet size attempted for MGCP-controlled connections, use the **mgcp playout** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
mgcp playout { adaptive init-value min-value max-value | fixed init-value }
```

```
no mgcp playout { adaptive | fixed }
```

### Syntax Description

<b>adaptive</b> <i>init-value min-value max-value</i>	Specifies a user-defined variable range (in milliseconds) for the jitter buffer packet size. The range for each value is 4 to 250. The default values are: <i>init-value</i> 60, <i>min-value</i> 4, and <i>max-value</i> 200. Note that <i>init-value</i> must be between <i>min-value</i> and <i>max-value</i> .
<b>fixed</b> <i>init-value</i>	Specifies a fixed size (in milliseconds) for the jitter buffer packet size. Valid values are from 4 to 250.

## mgcp quality-threshold

To set the jitter buffer size threshold, latency threshold, and packet-loss threshold parameters, use the **mgcp quality-threshold** command in global configuration mode. To restore the default parameter values, use the **no** form of this command.

```
mgcp quality-threshold { hwm-jitter-buffer value | hwm-latency value | hwm-packet-loss value  
| lwm-jitter-buffer value | lwm-latency value | lwm-packet-loss value }
```

```
no mgcp quality-threshold { hwm-jitter-buffer | hwm-latency | hwm-packet-loss |  
lwm-jitter-buffer | lwm-latency | lwm-packet-loss }
```

### Syntax Description

<b>hwm-jitter-buffer</b> <i>value</i>	Specifies the high-water-mark jitter buffer size. Valid range is from 100 to 200, and the default value is 150 milliseconds.
<b>hwm-latency</b> <i>value</i>	Specifies the high-water-mark latency value. Valid range is from 250 to 400 milliseconds, and the default value is 300 milliseconds.
<b>hwm-packet-loss</b> <i>value</i>	Specifies the high-water-mark packet-loss value. Valid range is from 5000 to 25,000 milliseconds, and the default value is 10000 milliseconds.
<b>lwm-jitter-buffer</b> <i>value</i>	Specifies the low-water-mark jitter buffer size. Valid range is from 4 to 60 milliseconds, and the default value is 30 milliseconds.
<b>lwm-latency</b> <i>value</i>	Specifies the low-water-mark latency value. Valid range is from 125 to 200 milliseconds, and the default value is 150 milliseconds.
<b>lwm-packet-loss</b> <i>value</i>	Specifies the low-water-mark packet-loss value. Valid range is from 1 to 3000 milliseconds, and the default value is 1000 milliseconds.

## mgcp request retries

To specify the number of times to retry sending the **mgcp** command, use the **mgcp request retries** command in global configuration mode. To restore the default value, use the **no** form of this command.

**mgcp request retries** *count*

**no mgcp request retries**

<b>Syntax Description</b>	<i>count</i>	Specifies the number of times a Notify message is resent to the Call Agent before the request is dropped. The valid range is 1 to 10.
---------------------------	--------------	---

## mgcp request timeout

To specify how long the system waits for a response to a request, use the **mgcp request timeout** command in global configuration mode. To restore the default value, use the **no** form of this command.

**mgcp request timeout** *timeout*

**no mgcp request timeout**

<b>Syntax Description</b>	<i>timeout</i>	Specifies the number of milliseconds to wait for a response to a request. The valid range is 1 to 10,000 (10 seconds).
---------------------------	----------------	--

## mgcp restart-delay

To select the delay value sent in the Restart in Progress (RSIP) graceful teardown, use the **mgcp restart-delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

**mgcp restart-delay** *seconds*

**no mgcp restart-delay**

<b>Syntax Description</b>	<i>seconds</i>	Specifies the restart delay value in seconds. The valid range is from 0 to 600.
---------------------------	----------------	---

## mgcp sdp simple

To initiate a subset of the SDP protocol, use the **mgcp sdp simple** command in controller configuration mode. To return to the full set of SDP protocol fields, use the **no** form of this command.

**mgcp sdp simple**

**no mgcp sdp simple**

---

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

## mgcp vad

To set the default voice activity detection (VAD) parameter for MGCP, use the **mgcp vad** command in global configuration mode. To disable the VAD parameter, use the **no** form of this command.

**mgcp vad**

**no mgcp vad**

---

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

## microcode reload controller

To reload the firmware and FPGA from the command-line interface (CLI) without reloading the Cisco IOS image, use the **microcode reload controller** command in privileged EXEC mode.

**microcode reload controller** {t1 | e1} {x/y}

---

<b>Syntax Description</b>	<b>t1</b>	Specifies T1.
	<b>e1</b>	Specifies E1.
	<i>x/</i>	Controller slot number.
	<i>y</i>	Controller unit number.

---

## mmpip aaa global-password

To define a password to be used with CiscoSecure for Windows NT when using store and forward fax, use the **mmpip aaa global-password** command in global configuration mode. To restore the default state, use the **no** form of this command.

**mmpip aaa global-password** *password*

**no mmpip aaa global-password** *password*

<b>Syntax Description</b>	<i>password</i>	Character string used to define the password for CiscoSecure for Windows NT to be used with store and forward fax. The maximum length is 64 alphanumeric characters.
---------------------------	-----------------	--

## mmoip aaa method fax accounting

To define the name of the method list to be used for AAA accounting with store and forward fax, use the **mmoip aaa method fax accounting** command in global configuration mode. To restore the default value, use the **no** form of this command.

**mmoip aaa method fax accounting** *method-list-name*

**no mmoip aaa method fax accounting** *method-list-name*

<b>Syntax Description</b>	<i>method-list-name</i>	Character string used to name a list of accounting methods to be used with store and forward fax.
---------------------------	-------------------------	---

## mmoip aaa method fax authentication

To define the name of the method list to be used for AAA authentication with store and forward fax, use the **mmoip aaa method fax authentication** command in global configuration mode. To restore the default state, use the **no** form of this command.

**mmoip aaa method fax authentication** *method-list-name*

**no mmoip aaa method fax authentication** *method-list-name*

<b>Syntax Description</b>	<i>method-list-name</i>	Character string used to name a list of authentication methods to be used with store and forward fax.
---------------------------	-------------------------	---

## mmoip aaa receive-accounting enable

To enable on-ramp AAA accounting services, use the **mmoip aaa receive-accounting enable** command in global configuration mode. To restore the default state, use the **no** form of this command.

**mmoip aaa receive-accounting enable**

**no mmoip aaa receive-accounting enable**

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

## mmoip aaa receive-authentication enable

To enable on-ramp AAA authentication services, use the **mmoip aaa receive-authentication enable** command in global configuration mode. To restore the default state, use the **no** form of this command.

**mmoip aaa receive-authentication enable**

**no mmoip aaa receive-authentication enable**

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

## mmoip aaa receive-id primary

To specify the primary location where AAA retrieves its account identification information for on-ramp faxing, use the **mmoip aaa receive-id primary** command in global configuration mode. To restore the default state, which means that the account identification source is undefined, use the **no** form of this command.

**mmoip aaa receive-id primary { ani | dnis | gateway | redialer-id | redialer-dnis }**

**no mmoip aaa receive-id primary { ani | dnis | gateway | redialer-id | redialer-dnis }**

Syntax Description		
<b>ani</b>	Indicates that AAA uses the calling party telephone number (automatic number identification or ANI) as the AAA account identifier.	
<b>dnis</b>	Indicates that AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier.	
<b>gateway</b>	Indicates that AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: <i>router-name.domain-name</i> .	
<b>redialer-id</b>	Indicates that AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.	
<b>redialer-dnis</b>	Indicates that AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier captured by the redialer if a redialer device is present.	

## mmoip aaa receive-id secondary

To specify the secondary location where AAA retrieves its account identification information for on-ramp faxing if the primary identifier has not been defined, use the **mmoip aaa receive-id secondary** command in global configuration mode. To restore the default state, which means that the account identification source is undefined, use the **no** form of this command.

**mmoip aaa receive-id secondary { ani | dnis | gateway | redialer-id | redialer-dnis }**

**no mmoip aaa receive-id secondary { ani | dnis | gateway | redialer-id | redialer-dnis }**

Syntax Description		
<b>ani</b>	Indicates that AAA uses the calling party telephone number (automatic number identification or ANI) as the AAA account identifier.	
<b>dnis</b>	Indicates that AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier.	
<b>gateway</b>	Indicates that AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: <i>router-name.domain-name</i> .	
<b>redialer-id</b>	Indicates that AAA uses the account string returned by the external redialer device as the AAA account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.	
<b>redialer-dnis</b>	Indicates that AAA uses the called party telephone number (dialed number identification service or DNIS) as the AAA account identifier captured by the redialer if a redialer device is present.	

## mmoip aaa send-accounting enable

To enable off-ramp AAA accounting services, use the **mmoip aaa send-accounting enable** command in global configuration mode. To restore the default state, use the **no** form of this command.

**mmoip aaa send-accounting enable**

**no mmoip aaa send-accounting enable**

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

## mmoip aaa send-authentication enable

To enable off-ramp AAA authentication services, use the **mmoip aaa send-authentication enable** command in global configuration mode. To restore the default value, use the **no** form of this command.

**mmoip aaa send-authentication enable**

**no mmoip aaa send-authentication enable**

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

## mmoip aaa send-id primary

To specify the primary location where AAA retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id primary** command in global configuration mode. To restore the default state, which means that account identification source is undefined, use the **no** form of this command.

**mmoip aaa send-id primary {account-id | envelope-from | envelope-to | gateway}**

**no mmoip aaa send-id primary {account-id | envelope-from | envelope-to | gateway}**

Syntax Description		
	<b>account-id</b>	Indicates that AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the X-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
	<b>envelope-from</b>	Indicates that AAA uses the account username from the fax-mail header as the AAA account identifier.
	<b>envelope-to</b>	Indicates that AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
	<b>gateway</b>	Indicates that AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: <i>router-name.domain-name</i> .

## mmoip aaa send-id secondary

To specify the secondary location where AAA retrieves its account identification information for off-ramp faxing, use the **mmoip aaa send-id secondary** command in global configuration mode. To restore the default state, which means that account identification source is undefined, use the **no** form of this command.

```
mmoip aaa send-id secondary {account-id | envelope-from | envelope-to | gateway}
```

```
no mmoip aaa send-id secondary {account-id | envelope-from | envelope-to | gateway}
```

Syntax Description		
	<b>account-id</b>	Indicates that AAA uses the account username from the originating fax-mail system as the AAA account identifier. This means that the off-ramp gateway uses the account identifier in the x-account ID field of the e-mail header. Using this attribute offers end-to-end authentication and accounting tracking.
	<b>envelope-from</b>	Indicates that AAA uses the account username from the fax-mail header as the AAA account identifier.
	<b>envelope-to</b>	Indicates that AAA uses the recipient derived from the fax-mail header as the AAA account identifier.
	<b>gateway</b>	Indicates that AAA uses the router-specific name derived from the host name and domain name as the AAA account identifier, displayed in the following format: <i>router-name.domain-name</i> .

## mode

To set the mode of the T1/E1 controller and enter specific configuration commands for each mode type, use the **mode** command in controller configuration mode. To restore the default mode of the controller, use the **no** form of this command.

```
mode {atm | cas}
```

```
no mode {atm | cas}
```

Syntax Description		
	<b>atm</b>	Places the controller into ATM mode and creates an ATM interface (ATM 0) on the Cisco MC3810 multiservice concentrator. When ATM mode is enabled, no channel groups, channel-associated signaling (CAS) groups, CCS groups, or clear channels are allowed because ATM occupies all the DS0s on the T1/E1 trunk.  When you set the controller to ATM mode, the controller framing is automatically set to ESF for T1 or CRC4 for E1. The linecode is automatically set to B8ZS for T1 or HDBC for E1. When you remove ATM mode by entering the <b>no mode atm</b> command, ATM interface 0 is deleted.  ATM mode is supported only on controller 0 (T1 or E1 0).
	<b>cas</b>	Places the controller into CAS mode, which allows you to create channel groups, CAS groups, and clear channels (both data and CAS modes).  CAS mode is supported on both controller 0 and controller 1.

## mode ccs

To configure the T1/E1 controller to support CCS cross-connect or CCS frame forwarding, use the **mode ccs** command in controller configuration mode. To disable support for CCS cross-connect or CCS frame forwarding on the controller, use the **no** form of this command.

```
mode ccs { cross-connect | frame-forwarding }
```

```
no mode ccs { cross-connect | frame-forwarding }
```

Syntax Description		
	<b>cross-connect</b>	Enables CCS cross-connect on the controller.
	<b>frame-forwarding</b>	Enables CCS frame forwarding on the controller.

## modem passthrough (dial-peer)

To configure modem pass-through over VoIP for a specific dial peer, use the **modem passthrough** command in dial-peer configuration mode. To disable modem pass-through for a specific dial peer, use the **no modem passthrough** command.

```
modem passthrough { system | nse [payload-type number] codec { g711ulaw | g711alaw } [redundancy] }
```

```
no modem passthrough
```

Syntax Description		
	<b>system</b>	Defaults to the global configuration.
	<b>nse</b>	Named signaling event.
	<b>payload-type</b>	(Optional) NSE payload.
	<i>number</i>	(Optional) The value of the payload type (96–119).

<b>codec</b>	Voice compression for speech or audio signals. Codec selections for upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls, and then slow down when there is only voice traffic.
<b>g711ulaw</b>	Codec G.711 u-Law 64000 bits per second for T1.
<b>g711alaw</b>	Codec G.711 A-Law 64000 bits per second for E1.
<b>redundancy</b>	(Optional) Packet redundancy (RFC 2198) for modem traffic.

## modem passthrough (voice-service)

To configure modem passthrough over VoIP for the Cisco AS5300 universal access server, use the **modem passthrough** command in voice-service configuration mode. To disable modem pass-through, use the **no** form of this command.

```
modem passthrough nse [payload-type number] codec {g711ulaw | g711alaw}
[redundancy] [maximum-sessions value]
```

```
no modem passthrough
```

Syntax Description	
<b>nse</b>	Named signaling event.
<b>payload-type</b>	(Optional) NSE payload type.
<i>number</i>	(Optional) The value of the payload type. The number can be from 96 to 119.
<b>codec</b>	Codec selections for upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
<b>g711ulaw</b>	Codec G.711 u-Law 64000 bits per second for T1.
<b>g711alaw</b>	Codec G.711 A-Law 64000 bits per second for E1.
<b>redundancy</b>	(Optional) Packet redundancy (RFC 2198) for modem traffic.
<b>maximum-sessions</b>	(Optional) Maximum number of simultaneous modem pass-through sessions.
<i>value</i>	(Optional) The number of simultaneous modem pass through sessions. The minimum value is 1, and the maximum value is 26. The default is 16 sessions.

## mta receive aliases

To specify a host name accepted as an SMTP alias for off-ramp faxing, use the **mta receive aliases** command in global configuration mode. To disable this alias, use the **no** form of this command.

```
mta receive aliases string
```

```
no mta receive aliases string
```

<b>Syntax Description</b>	<i>string</i>	Specifies the host name or IP address to be used as an alias for the SMTP server. If you specify an IP address to be used as an alias, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
---------------------------	---------------	---

## mta receive generate-mdn

To specify that the off-ramp gateway process a response message disposition notice (MDN) from an SMTP server, use the **mta receive generate-mdn** command in global configuration mode. To disable message delivery notice generation, use the **no** form of this command.

**mta receive generate-mdn**

**no mta receive generate-mdn**

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

## mta receive maximum-recipients

To specify the maximum number of recipients for all SMTP connections, use the **mta receive maximum-recipients** command in global configuration mode. To restore the default value, use the **no** form of this command.

**mta receive maximum-recipients** *number*

**no mta receive maximum-recipients**

<b>Syntax Description</b>	<i>number</i>	Specifies the maximum number of recipients for all SMTP connections. Valid entries are from 0 to 1024.
---------------------------	---------------	--

## mta send mail-from

To specify the mail-from address (also called the RFC 821 envelope-from address or the Return-Path address), use the **mta send mail-from** command in global configuration mode. To disable this return path information, use the **no** form of this command.

**mta send mail-from** { **hostname** *string* | **username** *string* | **username** **\$\$** }

**no mta send mail-from** { **hostname** *string* | **username** *string* | **username** **\$\$** }

<b>Syntax Description</b>	<b>hostname</b> <i>string</i>	Text string that specifies the SMTP host name or IP address. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
	<b>username</b> <i>string</i>	Text string that specifies the sender username.
	<b>username</b> <b>\$\$</b>	Wildcard that specifies that the username will be derived from the calling number.

## mta send origin-prefix

To add information to the e-mail prefix header, use the **mta send origin-prefix** command in global configuration mode. To disable the defined string, use the **no** form of this command.

**mta send origin-prefix** *string*

**no mta send origin-prefix** *string*

<b>Syntax Description</b>	<i>string</i>	Text string that adds comments to the e-mail prefix header. If this string contains more than one word, the string value should be contained within quotation marks (“”).
---------------------------	---------------	---

## mta send postmaster

To define where an e-mail message should be delivered (the mail server postmaster account) if it cannot be delivered to the defined destination, use the **mta send postmaster** command in global configuration mode. To disable this defined postmaster, use the **no** form of this command.

**mta send postmaster** *e-mail-address*

**no mta send postmaster** *e-mail-address*

<b>Syntax Description</b>	<i>e-mail-address</i>	E-mail address that defines where this e-mail message should be delivered (the mail server postmaster account) if it cannot be delivered to the defined destination.
---------------------------	-----------------------	--

## mta send return-receipt-to

To specify the address where message disposition notices (MDNs) are sent, use the **mta send return-receipt-to** command in global configuration mode. To restore the default value, use the **no** form of this command.

**mta send return-receipt-to** {*hostname string* | *username string* | *username \$\$*}

**no mta send return-receipt-to** {*hostname string* | *username string* | *username \$\$*}

<b>Syntax Description</b>	<b>hostname</b> <i>string</i>	Text string that specifies the SMTP host name or IP address where MDNs are sent. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
	<b>username</b> <i>string</i>	Text string that specifies the sender username where MDNs are sent.
	<b>username</b> <i>\$\$</i>	Wildcard that specifies that the username are derived from the calling number.

## mta send server

To specify a destination mail server or servers, use the **mta send server** command in global configuration mode. To disable the specified destination mail server, use the **no** form of this command.

**mta send server** *{host-name | IP-address}*

**no mta send server** *{host-name | IP-address}*

---

### Syntax Description

<i>host-name</i>	Defines the host name of the destination mail server.
<i>IP-address</i>	Defines the IP address of the destination mail server.

---

## mta send subject

To specify the subject header of the e-mail message, use the **mta send subject** command in global configuration mode. To disable this string, use the **no** form of this command.

**mta send subject** *string*

**no mta send subject** *string*

---

### Syntax Description

<i>string</i>	Text string that specifies the subject header of an e-mail message.
---------------	---

---

## music-threshold

To specify the threshold for on-hold music for a specified voice port, use the **music-threshold** command in voice-port configuration mode. To disable this feature, use the **no** form of this command.

**music-threshold** *number*

**no music-threshold** *number*

---

### Syntax Description

<i>number</i>	The on-hold music threshold in decibels (dB). Valid entries are any integer from -70 to -30.
---------------	--

---

## network-clock base-rate

To configure the network clock base rate for universal I/O serial ports 0 and 1 on the Cisco MC3810 multiservice concentrator, use the **network-clock base-rate** command in global configuration mode. To disable the current network clock base rate, use the **no** form of this command.

**network-clock base-rate** {**56k** | **64k**}

**no network-clock base-rate** {**56k** | **64k**}

<b>Syntax Description</b>	<b>56k</b>	Sets the network clock base rate to 56 kbps.
	<b>64k</b>	Sets the network clock base rate to 64 kbps.

## network-clock-switch

To configure the switch delay time to the next priority network clock source when the current network clock source fails, use the **network-clock-switch** command in global configuration mode. To cancel the network clock delay time selection, use the **no** form of this command.

**network-clock-switch** [*switch-delay* | **never**] [*restore-delay* | **never**]

**no network-clock-switch**

<b>Syntax Description</b>	<i>switch-delay</i>	(Optional) The delay time, in seconds, before the next priority network clock source is used when the current network clock source fails. The range is from 0 to 99 seconds. The default is 10 seconds.
	<b>never</b>	(Optional) Indicates no delay time before the current network clock source recovers.
	<i>restore-delay</i>	(Optional) The delay time before the current network clock source recovers. The range is from 0 to 99 seconds.
	<b>never</b>	(Optional) Indicates no delay time, in seconds, before the next priority network clock source is used when the current network clock source fails.

## non-linear

To enable nonlinear processing in the echo canceller, use the **non-linear** command in voice-port configuration mode. To disable nonlinear processing, use the **no** form of this command.

**non-linear**

**no non-linear**

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

## nsap

To specify the network service access point (NSAP) address for a local video dial peer, use the **nsap** command in dial-peer configuration mode. To remove any configured NSAP address from the dial peer, use the **no** form of this command.

**nsap** *nsap-address*

**no nsap**

<b>Syntax Description</b>	<i>nsap-address</i>	A 40-digit hexadecimal number; the number must be unique on the device.
---------------------------	---------------------	---

## num-exp

To define how to expand a telephone extension number into a particular destination pattern, use the **num-exp** command in global configuration mode. To cancel the configured number expansion, use the **no** form of this command.

**num-exp** *extension-number expanded-number*

**no num-exp** *extension-number*

### Syntax Description

<i>extension-number</i>	Digit or digits that define an extension number for a particular dial peer.
<i>expanded-number</i>	Digit or digits that define the expanded telephone number or destination pattern for the extension number listed.

## numbering-type

To match on a number type for a dial-peer call leg, use the **numbering-type** command in dial-peer configuration mode. To remove the numbering type for a dial-peer call leg, use the **no** form of this command.

**numbering-type** { **international** | **abbreviated** | **national** | **network** | **reserved** | **subscriber** | **unknown** }

**no numbering-type** { **international** | **abbreviated** | **national** | **network** | **reserved** | **subscriber** | **unknown** }

### Syntax Description

<b>international</b>	Specifies international numbering type.
<b>abbreviated</b>	Specifies abbreviated numbering type.
<b>national</b>	Specifies national numbering type.
<b>network</b>	Specifies network numbering type.
<b>reserved</b>	Specifies reserved numbering type.
<b>subscriber</b>	Specifies subscriber numbering type.
<b>unknown</b>	Specifies if the numbering type is unknown.

## operation

To select a specific cabling scheme for E&M ports, use the **operation** command in voice-port configuration mode. To restore the default, use the **no** form of this command.

**operation** { **2-wire** | **4-wire** }

**no operation** { **2-wire** | **4-wire** }

<b>Syntax Description</b>	<b>2-wire</b>	Specifies a 2-wire E&M cabling scheme.
	<b>4-wire</b>	Specifies a 4-wire E&M cabling scheme.

## output attenuation

To configure a specific output attenuation value, use the **output attenuation** command in voice-port configuration mode. To disable the selected output attenuation value, use the **no** form of this command.

**output attenuation** *decibels*

**no output attenuation**

<b>Syntax Description</b>	<i>decibels</i>	The amount of attenuation, in decibels, at the transmit side of the interface. An acceptable value is any integer from -6 to 14.
---------------------------	-----------------	--

## playout-delay

To tune the playout buffer on digital signal processors (DSPs) to accommodate packet jitter caused by switches in the WAN, use the **playout-delay** command in dial-peer configuration mode. To restore the default value, use the **no** form of this command.

**playout-delay** { **nominal** *milliseconds* | **maximum** *milliseconds* | **minimum** { **default** | **low** | **high** } }

**no playout-delay** { **nominal** *milliseconds* | **maximum** *milliseconds* | **minimum** { **default** | **low** | **high** } }

<b>Syntax Description</b>	<b>nominal</b> <i>milliseconds</i>	<p>The <b>nominal</b> keyword represents the amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway. In fixed mode, this is also the maximum size of the jitter buffer throughout the call.</p> <p>The <i>milliseconds</i> argument is the number of milliseconds (ms) of delay; the range accepted is from 0 to 1500, although this value depends on the type of DSP and how the voice card is configured for codec complexity. (See the <b>codec complexity</b> command.)</p> <p>If the voice card is configured for high codec complexity, the highest value that can be configured for <b>nominal</b> for compressed codecs is 250 ms. For medium-complexity codec configurations, the highest <b>nominal</b> value is 150 ms.</p> <p>Voice hardware that does not support the voice card complexity configuration (such as analog voice modules for the Cisco 3600 series router) has an upper limit of 250 ms.</p>
---------------------------	------------------------------------	--

---

**maximum** *milliseconds* (Adaptive mode only)

The **maximum** keyword represents the upper limit of the jitter buffer, or the highest value to which the adaptive delay will be set.

The *milliseconds* argument is the number of milliseconds of delay; the range accepted is from 40 to 1700, although this value depends on the type of DSP and how the voice card is configured for codec complexity. (See the **codec complexity** command.)

If the voice card is configured for high codec complexity, the highest value that can be configured for **maximum** for compressed codecs is 250 ms. For medium-complexity codec configurations, the highest **maximum** value is 150 ms.

Voice hardware that does not support the voice card complexity configuration (such as analog voice modules for the Cisco 3600 series router) has an upper limit of 250 ms.

---

**minimum** (Adaptive mode only)

The **minimum** keyword represents the lower limit of the jitter buffer, or the lowest value to which adaptive delay will be set.

The **low** keyword represents 10 milliseconds. Use this keyword when there are low jitter conditions in the network.

The **high** keyword represents 80 milliseconds. Use this keyword when there are high jitter conditions in the network.

The **default** keyword represents 40 milliseconds and is appropriate when there are normal jitter conditions in the network. This is the default value used in adaptive mode when a minimum value is not configured.

---

## playout-delay (voice-port)

To tune the playout buffer to accommodate packet jitter caused by switches in the WAN, use the **playout-delay** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**playout-delay** { **maximum** | **nominal** } *milliseconds*

**no playout-delay** { **maximum** | **nominal** }

---

**Syntax Description**

<b>maximum</b>	The delay time that the DSP allows before starting to discard voice packets. The default is 160 milliseconds.
<b>nominal</b>	The initial (and minimum allowed) delay time that the DSP inserts before playing out voice packets. The default is 80 milliseconds.
<i>milliseconds</i>	Playout-delay value, in milliseconds. The range for maximum playout delay is 40 to 320, and the range for nominal playout delay is 40 to 240.

---

## playout-delay mode

To select fixed or adaptive mode for playout delay from the jitter buffer on digital signal processors (DSPs), use the **playout-delay mode** command in dial-peer configuration mode or voice port configuration mode. To restore the default value, use the **no** form of this command.

```
playout-delay mode {adaptive | fixed [no-timestamps]}
```

```
no playout-delay mode {adaptive | fixed [no-timestamps]}
```

Syntax Description		
	<b>adaptive</b>	Jitter buffer size and amount of playout delay are adjusted during a call, on the basis of current network conditions.
	<b>fixed</b>	Jitter buffer size does not adjust during a call; a constant playout delay is added.
	<b>no-timestamps</b>	(Optional)No longer used; included for backward compatibility only. Formerly set the jitter buffer at a constant delay without reading Real-Time Transport Protocol (RTP) time stamps.

## port (dial peer)

To associate a dial peer with a specific voice port, use the **port** command in dial-peer configuration mode. To cancel this association, use the **no** form of this command.

### Cisco 1750 Router

```
port slot-number/port
```

```
no port slot-number/port
```

### Cisco 2600 and 3600 Series Routers

```
port {slot-number/subunit-number/port} | {slot/port:ds0-group-no}
```

```
no port {slot-number/subunit-number/port} | {slot/port:ds0-group-no}
```

### Cisco MC3810 Multiservice Concentrator

```
port slot/port
```

```
no port slot/port
```

### Cisco AS5300 Universal Access Server

```
port controller number:D
```

```
no port controller number:D
```

**Cisco AS5800 Universal Gateway**

**port** {shelf/slot/port:D} | {shelf/slot/parent:port:D}

**no port** {shelf/slot/port:D} | {shelf/slot/parent:port:D}

**Cisco 7200 Series Routers**

**port** {slot/port:ds0-group-no} | {slot-number/subunit-number/port}

**no port** {slot/port:ds0-group-no} | {slot-number/subunit-number/port}

**Syntax Description****For the Cisco 1750 Router**

<i>slot-number</i>	Slot number in the router in which the VIC is installed. Valid entries are from 0 to 2, depending on the slot in which it has been installed.
<i>port</i>	Voice port number. Valid entries are 0 or 1.

**For the Cisco 2600 and 3600 Series Routers**

<i>slot-number</i>	Slot number in the Cisco router where the voice interface card is installed. Valid entries are from 0 to 3, depending on the slot where it has been installed.
<i>subunit-number</i>	Subunit on the voice interface card where the voice port is located. Valid entries are 0 or 1.
<i>port</i>	Voice port number. Valid entries are 0 or 1.
<i>slot</i>	Router location where the voice port adapter is installed. Valid entries are from 0 to 3.
<i>port</i>	Voice interface card location. Valid entries are 0 or 3.
<i>dso-group-no</i>	Indicates the defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

**For the Cisco MC3810 Multiservice Concentrator**

<i>slot/port</i>	The <i>slot</i> variable specifies the slot number in the Cisco router where the voice interface card is installed. The only valid entry is 1.  The <i>port</i> variable specifies the voice port number. Valid ranges are as follows:  Analog voice ports: from 1 to 6.  Digital T1: from 1 to 24.  Digital E1: from 1 to 15, and from 17 to 31.
------------------	---

**For the Cisco AS5300 Universal Access Server**

<i>controller number</i>	Specifies the T1 or E1 controller.
<b>:D</b>	Indicates the D channel associated with ISDN PRI.

**For the Cisco AS5800 Universal Gateway**

<i>shelf/slot/port</i>	Specifies the T1 or E1 controller on the T1 card. Valid entries for the <i>shelf</i> variable is 0 to 9999. Valid entries for the <i>slot</i> value is 0 to 11. Valid entries for the <i>port</i> variable is 0 to 11.
<i>shelf/slot/parent:port</i>	Specifies the T1 controller on the T3 card. Valid entries for the <i>shelf</i> variable is 0 to 9999. Valid entries for the <i>slot</i> variable is 0 to 11. Valid entries for the <i>port</i> variable is 1 to 28. The value for the <i>parent</i> variable is always 0.
<b>:D</b>	Indicates the D channel associated with ISDN PRI.

**For the Cisco 7200 Series Routers**

<i>slot</i>	Router location where the voice port adapter is installed. Valid entries are from 0 to 3.
<i>port</i>	Voice interface card location. Valid entries are 0 or 1.
<i>dso-group-no</i>	Indicates the defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
<i>slot-number</i>	Indicates the slot number in the Cisco router where the voice interface card is installed. Valid entries are from 0 to 3, depending on the slot where it has been installed.
<i>subunit-number</i>	Indicates the subunit on the voice interface card where the voice port is located. Valid entries are 0 or 1.
<i>port</i>	Indicates the voice port number. Valid entries are 0 or 1.

## port media

To specify the serial interface to which the local video codec is connected for a local video dial peer, use the **port media** command in video dial-peer configuration mode. To remove any configured locations from the dial peer, use the **no** form of this command.

**port media** *interface*

**no port media**

**Syntax Description**

<i>interface</i>	Serial interface to which the local codec is connected. Valid entries are the numbers 0 or 1.
------------------	---

## port signal

To specify the slot location of the video dialing module (VDM) and the port location of the E1A/T1A RS-366 interface for signaling for a local video dial peer, use the **port signal** command in video dial-peer configuration mode. To remove any configured locations from the dial peer, use the **no** form of this command.

**port signal** *slot/port*

**no port signal**

**Syntax Description**

<i>slot/</i>	Slot location of the VDM. Valid values are 1 and 2.
<i>port</i>	Port location of the E1A/T1A RS-366 interface. The Cisco MC3810 multiservice concentrator VDM has only one port, so the <i>port</i> value is always 0.

## pots call-waiting

To enable the local call waiting feature on a Cisco 800 series router, use the global configuration **pots call-waiting** command in global configuration mode. To disable the local call waiting feature, use the **no** form of this command.

**pots call-waiting** {**local** | **remote**}

**no pots call-waiting** {**local** | **remote**}

**Syntax Description**

<b>local</b>	Enable call waiting on a local basis for the routers.
<b>remote</b>	Rely on the network provider service instead of the router to hold calls.

## pots country

To configure your connected telephones, fax machines, or modems to use country-specific default settings for each physical characteristic, use the **pots country** command in global configuration mode. To disable the use of country-specific default settings for each physical characteristic, use the **no** form of this command.

**pots country** *country*

**no pots country** *country*

**Syntax Description**

<i>country</i>	Specifies the country in which your router is.
----------------	--

## pots dialing-method

To specify how the router collects and sends digits dialed on your connected telephones, fax machines, or modems, use the **pots dialing-method** command in global configuration mode. To disable the specified dialing method, use the **no** form of this command.

**pots dialing-method** {**overlap** | **enblock**}

**no pots dialing-method** {**overlap** | **enblock**}

**Syntax Description**

<b>overlap</b>	The router sends each digit dialed in a separate message.
<b>enblock</b>	The router collects all digits dialed and sends the digits in one message.

## pots disconnect-supervision

To specify how a router notifies the connected telephones, fax machines, or modems when the calling party has disconnected, use the **pots disconnect-supervision** command in global configuration mode. To disable the specified disconnect method, use the **no** form of this command.

**pots disconnect-supervision** { *osi* | *reversal* }

**no pots disconnect-supervision** { *osi* | *reversal* }

Syntax Description		
<b>osi</b>	Open switching interval (OSI) is the duration for which DC voltage applied between tip and ring conductors of a telephone port is removed.	
<b>reversal</b>	Polarity reversal of tip and ring conductors of a telephone port.	

## pots disconnect-time

To specify the interval in which the disconnect method is applied if your connected telephones, fax machines, or modems fail to detect that a calling party has disconnected, use the **pots disconnect-time** command in global configuration mode. To disable the specified disconnect interval, use the **no** form of this command.

**pots disconnect-time** *interval*

**no pots disconnect-time** *interval*

Syntax Description	<i>interval</i>	Number from 50 to 2000 (milliseconds).

## pots distinctive-ring-guard-time

To specify the delay in which a telephone port can be rung after a previous call is disconnected, use the **pots distinctive-ring-guard-time** command in global configuration mode. To disable the specified delay, use the **no** form of this command.

**pots distinctive-ring-guard-time** *milliseconds*

**no pots distinctive-ring-guard-time** *milliseconds*

Syntax Description	<i>milliseconds</i>	Number from 0 to 1000 (milliseconds).

## pots encoding

To specify the pulse code modulation (PCM) encoding scheme for your connected telephones, fax machines, or modems, use the **pots encoding** command in global configuration mode. To disable the specified PCM encoding scheme, use the **no** form of this command.

```
pots encoding {alaw | ulaw}
```

```
no pots encoding {alaw | ulaw}
```

### Syntax Description

<b>alaw</b>	International Telecommunication Union Telecommunication Standardization Section (ITU-T) PCM encoding scheme used to represent analog voice samples as digital values.
<b>ulaw</b>	North American PCM encoding scheme used to represent analog voice samples as digital values.

## pots line-type

To specify the impedance of your connected telephones, fax machines, or modems, use the **pots line-type** command in global configuration mode. To disable the specified line type, use the **no** form of this command.

```
pots line-type {type1 | type2 | type3}
```

```
no pots line-type {type1 | type2 | type3}
```

### Syntax Description

<b>type1</b>	Runs at 600 ohms.
<b>type2</b>	Runs at 900 ohms.
<b>type3</b>	Runs at 300 or 400 ohms.

## pots ringing-freq

To specify the frequency on the Cisco 800 series router at which your connected telephones, fax machines, or modems ring, use the **pots ringing-freq** command in global configuration mode. To disable the specified ringing frequency, use the **no** form of this command.

```
pots ringing-freq {20Hz | 25Hz | 50Hz}
```

```
no pots ringing-freq {20Hz | 25Hz | 50Hz}
```

### Syntax Description

<b>20Hz</b>	Connected devices ring at 20 Hz.
<b>25Hz</b>	Connected devices ring at 25 Hz.
<b>50Hz</b>	Connected devices ring at 50 Hz.

## pots silence-time

To specify the interval of silence after a calling party disconnects, use the **pots silence-time** command in global configuration mode. To disable the specified silence time, use the **no** form of this command.

**pots silence-time** *interval*

**no pots silence-time** *interval*

<b>Syntax Description</b>	<i>interval</i>	Number from 0 to 10 (seconds).
---------------------------	-----------------	--------------------------------

## pots tone-source

To specify the source of dial, ringback, and busy tones for your connected telephones, fax machines, or modems, use the **pots tone-source** command in global configuration mode. To disable the specified tone source, use the **no** form of this command.

**pots tone-source** {**local** | **remote**}

**no pots tone-source** {**local** | **remote**}

<b>Syntax Description</b>	<b>local</b>	Router supplies the tones.
	<b>remote</b>	Telephone switch supplies the tones.

## pre-dial delay

To configure a delay on an Foreign Exchange Office (FXO) interface between the beginning of the off-hook state and the initiation of dual-tone multifrequency (DTMF) signaling, use the **pre-dial delay** command in voice-port configuration mode. To restore the default value, use the **no** form of the command.

**pre-dial delay** *seconds*

**no pre-dial delay**

<b>Syntax Description</b>	<i>seconds</i>	Delay, in seconds, before signaling begins. Valid values are from 0 to 10.
---------------------------	----------------	--

## preference

To indicate the preferred order of a dial peer within a hunt group, use the **preference** command in dial-peer configuration mode. To remove the preference value on the voice port, use the **no** form of this command.

**preference** *value*

**no preference** *value*

---

### Syntax Description

<i>value</i>	An integer from 0 to 10, where the lower the number, the higher the preference. The default value is 0 (highest preference).
--------------	--

---

## prefix

To specify the prefix of the dialed digits for a dial peer, use the **prefix** command in dial-peer configuration mode. To disable this feature, use the **no** form of this command.

**prefix** *string*

**no prefix**

---

### Syntax Description

<i>string</i>	Integers that represent the prefix of the telephone number associated with the specified dial peer. Valid numbers are 0 through 9, and a comma (.). Use a comma to include a pause in the prefix.
---------------	---

---

## pri-group

To specify an ISDN PRI on a channelized T1 or E1 controller, use the **pri-group** command in controller configuration mode. To remove the ISDN PRI configuration, use the **no** form of this command.

**pri-group timeslots** *timeslot-range*

**no pri-group**

---

### Syntax Description

<i>timeslot-range</i>	Specifies a single range of values. For T1, the allowable range is from 1 to 23. For E1, the allowable range is from 1 to 15.
-----------------------	---

---

## pri-group nec-fusion

To configure your NEC PBX to support Fusion Call Control Signaling (FCCS), use the **pri-group nec-fusion** command in controller configuration mode. To disable FCCS, use the **no** form of this command.

```
pri-group nec-fusion {pbx-ip-address | pbx-ip-host-name} pbx-port number
```

```
no pri-group nec-fusion {pbx-ip-address | pbx-ip-host-name} pbx-port number
```

Syntax Description	
<i>pbx-ip-address</i>	The IP address of the NEC PBX.
<i>pbx-ip-host-name</i>	The host name of the NEC PBX.
<i>number</i>	Choose a port number for the PBX. The range for the PBX port is 49152 to 65535. If you do not specify a port number, the default value of 55000 will be used. If this value is already in use, the next greater value will be used.

## progress\_ind

To set a specific progress indicator (PI) in call Setup, Progress, or Connect messages from an H.323 Voice over IP (VoIP) gateway, use the **progress\_ind** command in dial-peer configuration mode. To restore the default condition, use the **no** or **disable** forms of this command.

```
progress_ind {setup | connect | progress | alert} {enable pi-number | disable}
```

```
no progress_ind {setup | connect | progress | alert}
```



**Note** This command is not supported on VoIP gateways using session initiation protocol (SIP).

Syntax Description	
<b>setup</b>	Sets the progress indicator for Setup messages.
<b>connect</b>	Sets the progress indicator for Connect messages.
<b>progress</b>	Sets the progress indicator for Progress messages.
<b>alert</b>	Sets the progress indicator for Alert messages.
<b>enable</b>	Enables the configuration of the progress indicator.
<i>pi-number</i>	The progress indicator that is sent in all messages of the specified type from the outbound dial peer. For Setup messages from POTS or VoIP dial peers, values are 0, 1, or 3. For Progress, Connect, or Alert messages from a POTS dial peer, values are 1, 2, or 8.
<b>disable</b>	Disables the user configuration of the progress indicator.

# proxy h323

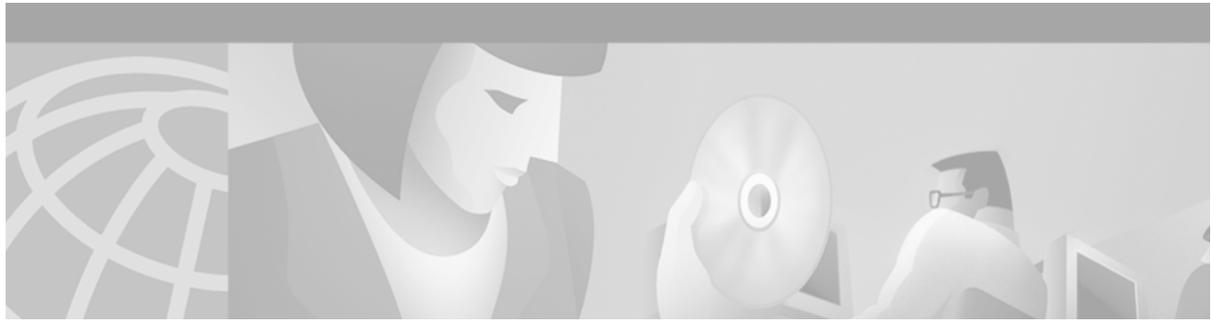
To enable the proxy feature on your router, use the **proxy h323** command in global configuration mode. To disable the proxy feature, use the **no** form of this command.

**proxy h323**

**no proxy h323**

---

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



## Voice, Video, and Fax Commands: register e164 Through shutdown (voice-port)

---

This chapter describes the function and syntax of the voice, video, and fax commands from **register e164** through **shutdown** (voice-port). For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Voice, Video, and Fax Command Reference*.

### register e164

To configure a gateway to register or deregister (remove the registration for) a fully qualified POTS dial-peer E.164 address with a gatekeeper, use the **register e164** command in dial-peer configuration mode. To deregister an E.164 address, use the **no** form of this command.

**register e164**

**no register e164**

---

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

### registered-caller ring

To configure the Nariwake service registered caller ring cadence, use the **registered-caller ring** command in dial-peer configuration mode.

**registered-caller ring** *cadence*

---

<b>Syntax Description</b>	<i>cadence</i>	A value of 0, 1, or 2. The default ring cadence for registered callers is 1 and for unregistered callers is 0. The on and off periods of ring 0 (normal ringing signals) and ring 1 (ringing signals for the Nariwake service) are defined in the NTT user manual.
---------------------------	----------------	--

---

## req-qos

To specify the desired quality of service to be used in reaching a specified dial peer, use the **req-qos** command in dial-peer configuration mode. To restore the default value for this command, use the **no** form of this command.

**req-qos** { **best-effort** | **controlled-load** | **guaranteed-delay** }

**no req-qos**

Syntax Description		
<b>best-effort</b>		Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation.
<b>controlled-load</b>		Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to assure that preferential service is received even when the bandwidth is overloaded.
<b>guaranteed-delay</b>		Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

## reset

To reset a set of digital signal processors (DSPs), use the **reset** command in global configuration mode.

**reset** *number*

Syntax Description	<i>number</i>	
		Specifies the number of DSPs to be reset. The number of DSPs ranges from 0 to 30.

## resource threshold

To configure a gateway to report H.323 resource availability to the its gatekeeper, use the **resource threshold** command in gateway configuration mode. To disable gateway resource-level reporting, use the **no** form of this command.

**resource threshold** [**all**] [**high** *percentage-value*] [**low** *percentage-value*]

**no resource threshold**

<b>Syntax Description</b>	<b>all</b>	(Optional) Applies the high- and low- parameter settings to all monitored H.323 resources. This is the default condition.
	<b>high</b> <i>percentage-value</i>	(Optional) A resource utilization level that triggers a Resource Availability Indicator (RAI) message indicating that H.323 resource use is high. Enter a number between 1 and 100 that represents the high-resource utilization percentage. A value of 100 specifies high-resource usage when any H.323 resource is unavailable. The default is 90 percent.
	<b>low</b> <i>percentage-value</i>	(Optional) Resource utilization level that triggers an RAI message indicating that H.323 resource usage has dropped below the high-usage level. Enter a number between 1 and 100 that represents the acceptable resource utilization percentage. After the gateway sends a high-utilization message, it waits to send the resource recovery message until the resource use drops below the value defined by the <b>low</b> parameter. The default is 90 percent.

## response-timeout

To configure the maximum time to wait for a response from a server, use the **response-timeout** command in settlement configuration mode. To restore the default value of this command, use the **no** form of this command.

**response-timeout** *number*

**no response-timeout** *number*

<b>Syntax Description</b>	<i>number</i>	Response waiting time in seconds.
---------------------------	---------------	-----------------------------------

## retry-delay

To set the time between attempts to connect with the settlement provider, use the **retry-delay** command in settlement configuration mode. To restore the default value, use the **no** form of this command.

**retry-delay** *number*

**no retry-delay**

<b>Syntax Description</b>	<i>number</i>	Length of time (in seconds) between attempts to connect with the settlement provider. The valid range for retry delay is from 1 to 600 seconds.
---------------------------	---------------	---

## retry-limit

To set the maximum number of attempts to connect to the provider, use the **retry-limit** command in settlement configuration mode. To restore the default value, use the **no** form of this command.

**retry-limit** *number*

**no retry-limit** *number*

---

### Syntax Description

<i>number</i>	Maximum number of connection attempts in addition to the first attempt.
---------------	---

---

## retry (SIP user-agent)

To configure the number of retry attempts for Session Initiation Protocol (SIP) messages, use the **retry** command in SIP user-agent configuration mode. To reset this command to the default value, use the **no** form of this command.

**retry** {**invite** *number* | **response** *number* | **bye** *number* | **cancel** *number*}

**no retry** {**invite** *number* | **response** *number* | **bye** *number* | **cancel** *number*}

---

### Syntax Description

<b>invite</b> <i>number</i>	Number of INVITE retries: 1 through 10 are valid inputs; default = 6.
<b>response</b> <i>number</i>	Number of RESPONSE retries: 1 through 10 are valid inputs; default = 6.
<b>bye</b> <i>number</i>	Number of BYE retries: 1 through 10 are valid inputs; default = 10.
<b>cancel</b> <i>number</i>	Number of CANCEL retries: 1 through 10 are valid inputs; default = 10.

---

## ring

To set up a distinctive ring for your connected telephones, fax machines, or modems, use the **ring** command in interface configuration mode. To disable the specified distinctive ring, use the **no** form of this command.

**ring** *cadence-number*

**no ring** *cadence-number*

---

### Syntax Description

<i>cadence-number</i>	Number from 0 through 2: <ul style="list-style-type: none"> <li>Type 0 is a primary ringing cadence—default ringing cadence for the country your router is in.</li> <li>Type 1 is a distinctive ring—0.8 seconds on, 0.4 seconds off, 0.8 seconds on, 0.4 seconds off.</li> <li>Type 2 is a distinctive ring—0.4 seconds on, 0.2 seconds off, 0.4 seconds on, 0.2 seconds off, 0.8 seconds on, 4 seconds off.</li> </ul>
-----------------------	--

---

# ring cadence

To specify the ring cadence for a Foreign Exchange Station (FXS) voice port, use the **ring cadence** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**ring cadence** {*pattern-number* | **define** *pulse interval*}

**no ring cadence**

## Syntax Description

<i>pattern-number</i>	Predefined ring cadence patterns. Each pattern specifies a ring-pulse time and a ring-interval time. <ul style="list-style-type: none"> <li><b>pattern01</b>—2 seconds on, 4 seconds off</li> <li><b>pattern02</b>—1 second on, 4 seconds off</li> <li><b>pattern03</b>—1.5 seconds on, 3.5 seconds off</li> <li><b>pattern04</b>—1 second on, 2 seconds off</li> <li><b>pattern05</b>—1 second on, 5 seconds off</li> <li><b>pattern06</b>—1 second on, 3 seconds off</li> <li><b>pattern07</b>—0.8 second on, 3.2 seconds off</li> <li><b>pattern08</b>—1.5 seconds on, 3 seconds off</li> <li><b>pattern09</b>—1.2 seconds on, 3.7 seconds off</li> <li><b>pattern09</b>—1.2 seconds on, 4.7 seconds off</li> <li><b>pattern11</b>—0.4 second on, 0.2 second off, 0.4 second on, 2 seconds off</li> <li><b>pattern12</b>—0.4 second on, 0.2 second off, 0.4 second on, 2.6 seconds off</li> </ul>
<b>define</b>	User-definable ring cadence pattern. Each number pair specifies one ring-pulse time and one ring-interval time. You must enter numbers in pairs, and you can enter from 1 to 6 pairs. The second number in the last pair that you enter specifies the interval between rings.
<i>pulse</i>	A number (1 or 2 digits) specifying ring pulse (on) time in hundreds of milliseconds.  The range is from 1 to 50, for pulses of 100 ms to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.
<i>interval</i>	A number (1 or 2 digits) specifying ring interval (off) time in hundreds of milliseconds.  The range is from 1 to 50, for pulses of 100 to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.

## ring frequency

To specify the ring frequency for a specified Foreign Exchange Station (FXS) voice port, use the **ring frequency** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**ring frequency** *number*

**no ring frequency** *number*

---

### Syntax Description

*number*

Ring frequency (hertz) used in the FXS interface. Valid entries on the Cisco 3600 series are 25 and 50. Valid entries on the Cisco MC3810 multiservice concentrator are 20 and 30.

---

## ring number

To specify the number of rings for a specified Foreign Exchange Office (FXO) voice port, use the **ring number** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**ring number** *number*

**no ring number** *number*

---

### Syntax Description

*number*

Number of rings detected before answering the call. Valid entries are numbers from 1 to 10. The default is 1.

---

## roaming

To enable the roaming capability for the dial peer, use the **roaming** command in dial-peer configuration mode. To disable the roaming capability, use the **no** form of this command.

**roaming**

**no roaming**

---

### Syntax Description

This command has no arguments or keywords.

## roaming (settlement)

To enable the roaming capability for a settlement provider, use the **roaming** command in settlement configuration mode. To disable the roaming capability, use the **no** form of this command.

**roaming**

**no roaming**

---

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

## rtsp client session history duration

To specify how long to keep Real Time Streaming Protocol (RTSP) session history records in memory, use the **rtsp client session history duration** command in global configuration mode. To set the value to the default, use the **no** form of this command.

**rtsp client session history duration** *number*

**no rtsp client session history duration** *number*

---

**Syntax Description** *number* Specifies how long, in minutes, to keep the record.

---

## rtsp client session history records

To configure the number of records to keep in the RTSP client session history, use the **rtsp client session history records** command in global configuration mode. To set the value to the default, use the **no** form of this command.

**rtsp client session history records** *number*

**no rtsp client session history records** *number*

---

**Syntax Description** *number* Specifies the number of records to retain in a session history. Values range from 1 to 100000.

---

## rule

To apply a translation rule to a calling party number or a called party number for both incoming and outgoing calls, use the **rule** command in translation-rule configuration mode. To remove the translation rule, use the **no** form of this command.

**rule** *name-tag input-matched-pattern substituted-pattern [match-type substituted-type]*

**no rule** *name-tag input-matched-pattern substituted-pattern [match-type substituted-type]*

**Syntax Description**

<i>name-tag</i>	The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. Range is from 1 through 2147483647.
<i>input-matched-pattern</i>	The input string of digits for which pattern matching is performed.
<i>substituted-pattern</i>	The replacement digit string that results after pattern matching is performed. Regular expressions are used to carry out this process.
<i>match-type</i>	(Optional) The choices for this field are <b>international</b> , <b>national</b> , <b>subscriber</b> , <b>abbreviated</b> , <b>unknown</b> , and <b>any</b> , as defined by the ITU Q.931 specification. If you enter the <i>match-type</i> value, then you must also enter the <i>substituted-type</i> value.
<i>substituted-type</i>	(Optional) The choices for this field are <b>international</b> , <b>national</b> , <b>subscriber</b> , <b>abbreviated</b> and <b>unknown</b> , as defined by the ITU Q.931 specification.

## security

To enable authentication and authorization on a gatekeeper, use the **security** command in gatekeeper configuration mode. To disable security, use the **no** form of this command.

```
security {any | h323-id | e164} {password default password | password separator character}
```

```
no security {any | h323-id | e164} {password default password | password separator character}
```

**Syntax Description**

<b>any</b>	Uses the first alias of an incoming RAS registration, regardless of its type, as the means of identifying the user to RADIUS/TACACS+.
<b>h323-id</b>	Uses the first H.323 ID type alias as the means of identifying the user to RADIUS/TACACS+.
<b>e164</b>	Uses the first E.164 address type alias as the means of identifying the user to RADIUS/TACACS+.
<b>password default</b> <i>password</i>	Specifies the default password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The <i>password</i> must be identical to the password on the authentication server.
<b>password separator</b> <i>character</i>	Specifies the character that endpoints use to separate the H.323-ID from the piggybacked password in the registration. Specifying this character allows each endpoint to supply a user-specific password. The separator character and password will be stripped from the string before it is treated as an H.323-ID alias to be registered.  Note that passwords may only be piggybacked in the H.323-ID, not the E.164 address, because the E.164 address allows a limited set of mostly numeric characters. If the endpoint does not wish to register an H.323-ID, it can still supply an H.323-ID consisting of just the separator character and password. This H.323-ID consisting of just the separator character and password will be understood to be a password mechanism and no H.323-ID will be registered.

## sequence-numbers

To enable the generation of sequence numbers in each frame generated by the digital signal processor (DSP) for Voice over Frame Relay applications, use the **sequence-numbers** command in dial-peer configuration mode. To disable the generation of sequence numbers, use the **no** form of this command.

**sequence-numbers**

**no sequence-numbers**

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

## server registration-port

To configure the listener port for the server to establish a connection with the gatekeeper, use the **server registration-port** command in gatekeeper configuration mode. To force the gatekeeper to close the listening socket so that no more new registration takes place, use the **no** form of this command. However, existing connections between the gatekeeper and the external applications are left open.

**server registration-port** *port number*

**no server registration-port** *port number*

<b>Syntax Description</b>	<i>port number</i>	Specifies a single range of values from 1 through 65535 for the port number on which the gatekeeper listens for external server connections.
---------------------------	--------------------	--

## server trigger

To configure a static server trigger for external applications, use the **server trigger** command in gatekeeper configuration mode. To remove a single statically configured trigger entry, use the **no** form of this command. To remove every static trigger you configured if you want to delete them all, use the **all** keyword.

**server trigger** {**arq** | **lcf** | **lrj** | **lrq** | **rrq** | **urq**} *gkid priority server-id server-ipaddress server-port*

**no server trigger** {**arq** | **lcf** | **lrj** | **lrq** | **rrq** | **urq**} *gkid priority*

**no server trigger all**

<b>Syntax Description</b>	<b>all</b>	Specified to delete all command-line interface configured triggers.
	<b>arq, lcf, lrj, lrq, rrq, urq</b>	RAS message types. Use these message types to specify a submode in the gatekeeper configuration mode in which you configure a trigger for the gatekeeper to act upon. Specify only one message type per server trigger command. There is a different trigger submode for each message type. Each trigger submode has its own set of applicable commands.

<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is from 1 through 20, with 1 being the highest priority.
<i>server-id</i>	The ID number of the external application.
<i>server-ipaddress</i>	The IP address of the server.
<i>server-port</i>	The port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

## session protocol

To specify a session protocol for calls between the local and remote routers using the packet network, use the **session protocol** command in dial-peer configuration mode. To reset the default value for this command, use the **no** form of this command.

```
session protocol { cisco | sipv2 | aal2-trunk | smtp }
```

```
no session protocol
```

### Syntax Description

<b>cisco</b>	Configure the dial peer to use proprietary Cisco VoIP session protocol.
<b>sipv2</b>	SIP users should use this option. This option configures the VoIP dial peer to use IETF SIP.
<b>aal2-trunk</b>	AAL2 nonswitched trunk session protocol.
<b>smtp</b>	Specifies Simple Mail Transfer Protocol (SMTP) session protocol.

## session protocol (Voice over Frame Relay)

To establish a Voice over Frame Relay protocol for calls between the local and remote routers via the packet network, use the **session protocol** command in dial-peer configuration mode. To reset the default value, use the **no** form of this command.

```
session protocol { cisco-switched | frf11-trunk }
```

```
no session protocol
```

### Syntax Description

<b>cisco-switched</b>	Specifies proprietary Cisco VoFR session protocol. (This is the only valid session protocol for the Cisco 7200 series.)
<b>frf11-trunk</b>	Specifies FRF.11 session protocol.

## session protocol aal2

To enter the voice-service-session configuration mode and specify AAL2 trunking on a Cisco MC3810 multiservice concentrator, use the **session protocol aal2** command in voice-service configuration mode.

```
session protocol aal2
```

---

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

## session protocol multicast

To set the session protocol as multicast, use the **session protocol multicast** command dial-peer configuration mode. To negate this command and return to the Cisco default session protocol, use the **no** version of this command.

```
session protocol multicast
```

```
no session protocol multicast
```

---

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

## session target

To specify a network-specific address for a specified dial peer, use the **session target** command in dial-peer configuration mode. To restore default values for this parameter, use the **no** form of this command.

**Note**

---

This command applies to all dial peers except POTS dial peers.

---

**Cisco 2600 and 3600 Series Routers Voice over Frame Relay Dial Peers**

```
session target interface dci [cid]
```

```
no session target
```

**Cisco 2600 and 3600 Series Routers and MC3810 Multiservice Concentrator Voice over IP Dial Peers**

```
session target {ipv4:destination-address | dns:[$$$. | $d$. | $e$. | $u$.] host-name |  
loopback:rtp | loopback:compressed | loopback:uncompressed }
```

```
no session target
```

**Cisco MC3810 Multiservice Concentrator Voice over Frame Relay Dial Peers**

```
session target interface dci [cid]
```

```
no session target
```

**Cisco 3600 Service Routers Voice over ATM Dial Peers**

```
session target interface pvc {name | vpi/vci | vci}
no session target
```

**Cisco MC3810 Multiservice Concentrator Voice over ATM Dial Peers**

```
session target {serial | atm} interface pvc {word | vpi/vci | vci} cid
no session target
```

**Cisco AS5300 Universal Access Servers Voice over IP Dial Peers**

```
session target {ipv4:destination-address | dns:[$$$. | $d$. | $e$. | $u$.] host-name |
loopback:rtp | loopback:compressed | loopback:uncompressed | mailto:{name |
$d$}@domain-name | ipv4:destination-address | dns:[$$$. | $d$. | $u$. | $e$.] host-name}
no session target
```

**Cisco AS5800 Universal Access Servers Voice over IP Dial Peers**

```
session target {ipv4:destination-address | dns:[$$$. | $d$. | $e$. | $u$.] host-name |
loopback:rtp | loopback:compressed | loopback:uncompressed}
no session target
```

**Cisco 7200 Series Routers Voice over Frame Relay Dial Peers**

```
session target interface dlci
no session target
```

**Syntax Description****For the Cisco 2600 and 3600 Series Routers Voice over Frame Relay Dial Peers**

<i>interface</i>	Specifies the serial interface and interface number (slot number and port number) associated with this dial peer.
<i>dlci</i>	Specifies the data link connection identifier for this dial peer. The valid range is from 16 to 1007.
<i>cid</i>	(Optional) Specifies the DLCI subchannel to be used for data on FRF.11 calls. A CID must be specified only when the session protocol is <b>frf11-trunk</b> . When the session protocol is <b>cisco-switched</b> , the CID is dynamically allocated. The valid range is from 4 to 255.

**Note**

By default, CID 4 is used for data; CID 5 is used for call-control. We recommend that you select CID values between 6 and 63 for voice traffic. If the CID is greater than 63, the FRF.11 header will contain an extra byte of data.

**For the Cisco 2600 and Cisco 3600 Series Routers Voice over IP Dial Peers**

<b>ipv4:destination-address</b>	IP address of the dial peer.
<b>dns:host-name</b>	<p>Indicates that the domain name server will be used to resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device.</p> <p>(Optional) You can use one of the following three wildcards with this keyword when defining the session target for Voice over IP (VoIP) peers:</p> <ul style="list-style-type: none"> <li>• <b>\$s\$</b>.—Indicates that the source destination pattern will be used as part of the domain name.</li> <li>• <b>\$d\$</b>.—Indicates that the destination number will be used as part of the domain name.</li> <li>• <b>\$e\$</b>.—Indicates that the digits in the called number will be reversed, periods will be added in between the digits of the called number, and this string will be used as part of the domain name.</li> <li>• <b>\$u\$</b>.—Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.</li> </ul>
<b>loopback:rtp</b>	Indicates that all voice data will be looped back to the source. This is applicable for VoIP peers.
<b>loopback:compressed</b>	Indicates that all voice data will be looped back in compressed mode to the source. This is applicable for POTS peers.
<b>loopback:uncompressed</b>	Indicates that all voice data will be looped back in uncompressed mode to the source. This is applicable for POTS peers.

**For the Cisco MC3810 Multiservice Concentrator Voice over Frame Relay Dial Peers**

<i>interface</i>	Specifies the interface type and interface number on the Cisco MC3810 multiservice concentrator. For the range of valid interface numbers for the selected interface type, enter a ? character after the interface type.
<i>dlci</i>	Specifies the Frame Relay DLCI. The valid range is from 16 to 1007.
<i>cid</i>	(Optional) Specifies a subchannel ID for the Frame Relay DLCI. The valid range is from 4 to 255.

**For the Cisco 3600 Series Routers Voice over ATM Dial Peers**

<i>interface</i>	Interface type and interface number on the router.
<b>pvc</b>	The specific ATM permanent virtual circuit (PVC) for this dial peer.
<i>word</i>	(Optional) A name that identifies the PVC. The argument can identify the PVC if a word identifier was assigned when the PVC was created.

<i>vpi/vci</i>	ATM network virtual path identifier (VPI) and virtual channel identifier (VCI) of this PVC.  On the Cisco 3600, if you have the Multiport T1/E1 ATM network module with IMA installed, the valid range for <i>vpi</i> is from 0 to 5, and the valid range for <i>vci</i> is from 1 to 255.  If you have the OC3 ATM Network Module installed, the valid range for <i>vpi</i> is from 0 to 15, and the valid range for <i>vci</i> is from 1 to 1023.
<i>vci</i>	ATM network virtual channel identifier (VCI) of this PVC.
<i>cid</i>	ATM network channel identifier (CID) of this PVC. The valid range is from 8 to 255.

**For the Cisco MC3810 Multiservice Concentrator Voice over ATM Dial Peers**

<b>serial</b>	Specifies the serial interface for the dial-peer address.
<b>atm</b>	Specifies the ATM interface. The only valid number is 0.
<i>interface</i>	Specifies the interface number.
<b>pvc</b>	Specifies a PVC.
<i>name</i>	The PVC name.
<i>vpi/vci</i>	The ATM network VPI and VCI of this PVC.
<i>vci</i>	The ATM network VCI of this PVC.

**For the Cisco AS5300 Universal Access Servers Voice over IP Dial Peers**

<b>mailto:name</b>	Specific recipient e-mail address, name, or mailing list alias.
<b>mailto</b>	Wildcard that inserts the destination pattern of the recipient.
<i>@domain-name</i>	Specifies the appropriate domain name associated with the e-mail address.
<b>ipv4:destination-address</b>	IP address of the dial peer.
<b>dns:host-name</b>	Indicates that the domain name server will be used to resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device.  (Optional) You can use one of the following three wildcards with this keyword when defining the session target for VoIP peers: <ul style="list-style-type: none"> <li>• <b>\$s\$</b>.—Indicates that the source destination pattern will be used as part of the domain name.</li> <li>• <b>\$d\$</b>.—Indicates that the destination number will be used as part of the domain name.</li> <li>• <b>\$e\$</b>.—Indicates that the destination pattern is used as part of the domain name in reverse dotted format for tpc.int DNS format. For example, if the destination number is 310 555-1234 and the session target is configured as <b>\$e\$.cisco.com</b>, the translated DNS name will be 4.3.2.1.5.5.5.0.1.3.cisco.com.</li> <li>• <b>\$u\$</b>.—Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.</li> </ul>

<b>loopback:rtp</b>	Indicates that all voice data will be looped back to the source. This applies to VoIP peers.
<b>loopback:compressed</b>	Indicates that all voice data will be looped back in compressed mode to the source. This applies to POTS peers.
<b>loopback:uncompressed</b>	Indicates that all voice data will be looped back in uncompressed mode to the source. This applies to POTS peers.

#### For the Cisco AS5800 Universal Access Servers Voice over IP Dial Peers

<b>ipv4:destination-address</b>	IP address of the dial peer.
<b>dns:host-name</b>	<p>Indicates that the domain name server will be used to resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device.</p> <p>(Optional) You can use one of the following three wildcards with this keyword when defining the session target for VoIP peers:</p> <ul style="list-style-type: none"> <li>• <b>\$s\$</b>.—Indicates that the source destination pattern will be used as part of the domain name.</li> <li>• <b>\$d\$</b>.—Indicates that the destination number will be used as part of the domain name.</li> <li>• <b>\$e\$</b>.—Indicates that the destination pattern is used as part of the domain name in reverse dotted format for tpc.int DNS format. For example, if the destination number is 310 555-1234 and the session target is configured as \$e\$.cisco.com, the translated DNS name will be 4.3.2.1.5.5.5.0.1.3.cisco.com.</li> <li>• <b>\$u\$</b>.—Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.</li> </ul>
<b>loopback:rtp</b>	Indicates that all voice data will be looped back to the source. This applies to VoIP peers.
<b>loopback:compressed</b>	Indicates that all voice data will be looped back in compressed mode to the source. This applies to POTS peers.
<b>loopback:uncompressed</b>	Indicates that all voice data will be looped back in uncompressed mode to the source. This applies to POTS peers.

#### Cisco 7200 Series Voice over Frame Relay Dial Peers

<i>interface</i>	Specifies the interface type and interface number on the Cisco 7200 series router. For the range of valid interface numbers for the selected interface type, enter a ? character after the interface type.
<i>dldci</i>	Specifies the Frame Relay DLCI. The valid range is from 16 to 1007.

## session target (VoIP)

To specify a network-specific address for a specified dial peer, use the **session target** command in dial-peer configuration mode. To restore default values for this parameter, use the **no** form of this command.



### Note

This command applies to all dial peers except POTS dial peers.

```
session target { ipv4:destination-address | dns:[$$$. | $d$. | $e$. | $u$.] host-name | loopback:rtp
| loopback:compressed | loopback:uncompressed | ras | settlement }
```

```
no session target { ipv4:destination-address | dns:[$$$. | $d$. | $e$. | $u$.] host-name |
loopback:rtp | loopback:compressed | loopback:uncompressed | ras | settlement }
```

### Syntax Description

<b>ipv4:destination-address</b>	IP address of the dial peer.
<b>dns:[\$\$\$.] host-name</b>	Indicates that the domain name server will be used to resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device.  (Optional) Use one of the following three wildcards with this keyword when defining the session target for Voice over IP (VoIP) peers:  <b>\$\$\$.</b> —Indicates that the source destination pattern will be used as part of the domain name.  <b>\$d\$.</b> —Indicates that the destination number will be used as part of the domain name.  <b>\$e\$.</b> —Indicates that the digits in the called number will be reversed, periods will be added between the digits of the called number, and this string will be used as part of the domain name.  <b>\$u\$.</b> —Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.
<b>loopback:rtp</b>	Indicates that all voice data will be looped back to the source. This is applicable for VoIP peers.
<b>loopback:compressed</b>	Indicates that all voice data will be looped back in compressed mode to the source. This is applicable for POTS peers.
<b>loopback:uncompressed</b>	Indicates that all voice data will be looped-back in uncompressed mode to the source. This is applicable for POTS peers.
<b>ras</b>	Indicates that the RAS signaling function protocol is being used, meaning that a gatekeeper will be consulted to translate the E.164 address into an IP address.
<b>settlement</b> <i>provider-number</i>	Indicates that the settlement server is the target to resolve the terminating gateway address. Enter the provider IP address for provider number.

## session transport

To configure the VoIP dial peer to use TCP or User Datagram Protocol (UDP) as the underlying transport layer protocol for Session Initiation Protocol (SIP) messages, use the **session transport** command in dial-peer configuration mode. To reset the value to the default, use the **no** form of this command.

```
session transport {udp | tcp }
```

Syntax Description	udp	tcp
	Configure the SIP dial peer to use the UDP transport layer protocol. This is the default.	Configure the SIP dial peer to use the TCP transport layer protocol.

## settle-call

To force a call to be authorized with a settlement server that uses the address resolution method specified in the **session target type** command, use the **settle-call** command in dial-peer configuration mode. To make sure that no authorization will be performed by a settlement server, use the **no** form of this command.

```
settle-call provider-number
```

```
no settle-call provider-number
```

Syntax Description	provider-number
	Digit defining the ID of a particular settlement server. The only valid entry is 0.

 **Note** If **session target type** is **settlement**, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

## settlement

To enter settlement configuration mode and specify the attributes specific to a settlement provider, use the **settlement** command in global configuration mode. To disable the settlement provider, use the **no** form of this command.

```
settlement provider-number
```

```
no settlement provider-number
```

Syntax Description	provider-number
	Specifies a digit that defines a particular settlement server. The only valid entry is 0.

## settlement roam-pattern

To configure a pattern that must be matched to determine if a user is roaming, use the **settlement roam-pattern** command in global configuration mode. To delete a particular pattern, use the **no** form of this command.

```
settlement provider-number roam-pattern pattern {roaming | no roaming}
```

```
no settlement provider-number roam-pattern pattern {roaming | no roaming}
```

### Syntax Description

<i>provider-number</i>	Digit defining the ID of particular settlement server. The only valid entry is 0.
<i>pattern</i>	Specifies a user account pattern.
<b>roaming   no roaming</b>	Determines whether a user is roaming.

## sgcp

To start and allocate resources for the Simple Gateway Control Protocol (SGCP) daemon, use the **sgcp** command in global configuration mode. To terminate all calls, release all allocated resources, and kill the SGCP daemon, use the **no** form of this command.

```
sgcp
```

```
no sgcp
```

### Syntax Description

This command has no arguments or keywords.

## sgcp call-agent

To define the IP address of the default SGCP call agent in the router configuration file, use the **sgcp call-agent** command in global configuration mode. To remove the IP address of the default SGCP call agent from the router configuration, use the **no** form of this command.

```
sgcp call-agent ipaddress [:udp port]
```

```
no sgcp call-agent ipaddress
```

### Syntax Description

<i>ipaddress</i>	Specifies the IP address or hostname of the call agent.
<i>:udp port</i>	(Optional) Specifies the UDP port of the call agent.

## sgcp graceful-shutdown

To block all new calls and gracefully terminate all existing calls (wait for the caller to end the call), use the **sgcp graceful-shutdown** command in global configuration mode. To unblock all calls and allow new calls to go through, use the **no** form of this command.

```
sgcp graceful-shutdown
```

```
no sgcp graceful-shutdown
```

---

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

## sgcp max-waiting-delay

To set the Simple Gateway Control Protocol (SGCP) maximum waiting delay to prevent restart avalanches, use the **sgcp max-waiting-delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
sgcp max-waiting-delay delay
```

```
no sgcp max-waiting-delay delay
```

---

<b>Syntax Description</b>	<i>delay</i>	Sets the maximum waiting delay (MWD) value in milliseconds. The valid range is from 0 to 600,000. The default is 3000.
---------------------------	--------------	--

---

## sgcp modem passthru

To enable Simple Gateway Control Protocol (SGCP) modem or fax pass-through, use the **sgcp modem passthru** command in global configuration mode. To disable SGCP modem or fax pass-through, use the **no** form of this command.

```
sgcp modem passthru {ca | cisco | nse}
```

```
no sgcp modem passthru {ca | cisco | nse}
```

---

<b>Syntax Description</b>	<b>ca</b>	Uses the call agent controlled modem upspeed method violation message.
	<b>cisco</b>	Uses a Cisco-proprietary upspeed method based on the protocol.
	<b>nse</b>	Uses the NSE-based modem upspeed method.

---

## sgcp quarantine-buffer disable

To disable the SGCP quarantine buffer, use the **sgcp quarantine-buffer disable** command in global configuration mode. To reenable the SGCP quarantine buffer, use the **no** form of this command.

**sgcp quarantine-buffer disable**

**no sgcp quarantine-buffer disable**

---

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

## sgcp request retries

To specify the number of times to retry sending “notify” and “delete” messages to the SGCP call agent, use the **sgcp request retries** command in global configuration mode. To restore the default value, use the **no** form of this command.

**sgcp request retries** *count*

**no sgcp request retries**

---

<b>Syntax Description</b>	<i>count</i>	Specifies the number of times a “notify” and “delete” message is retransmitted to the SGCP call agent before it is dropped. The valid range is from 1 to 100. The default is 3.
---------------------------	--------------	---

---

## sgcp request timeout

To specify how long the system should wait for a response to a request, use the **sgcp request timeout** command in global configuration mode. To restore the default value, use the **no** form of this command.

**sgcp request timeout** *timeout*

**no sgcp request timeout**

---

<b>Syntax Description</b>	<i>timeout</i>	Specifies the number of milliseconds to wait for a response to a request. Valid range is from 1 to 10,000.
---------------------------	----------------	--

---

## sgcp restart

To trigger the router to send a Restart in Progress (RSIP) message to the Simple Gateway Control Protocol (SGCP) call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller, use the **sgcp restart** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
sgcp restart {delay delay | notify}
```

```
no sgcp restart {delay delay | notify}
```

Syntax Description	delay delay	notify
	Specifies the restart delay timer value in milliseconds. The valid range is from 0 to 600, and the default value is 0.	Enables the restart notification upon the SGCP/digital interface state transition.

## sgcp retransmit timer

To configure the SGCP retransmission timer to use a random algorithm method, use the **sgcp retransmit timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
sgcp retransmit timer {random}
```

```
no sgcp retransmit timer {random}
```

Syntax Description	random
	Enables the SGCP retransmission timer to use a random algorithm method. This is the only keyword supported in this release.

## sgcp timer

To configure how the gateway detects the RTP stream lost, use the **sgcp timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
sgcp timer {receive-rtcp timer | rtp-nse timer}
```

```
no sgcp timer {receive-rtcp timer | rtp-nse timer}
```

Syntax Description	receive-rtcp timer	rtp-nse timer
	Sets the multiples of the RTCP transmission interval in milliseconds. The valid range is from 1 to 100, and the default is 5.	Sets the multiples of the RTP NSE timeout in milliseconds. The valid range is from 100 to 3000, and the default is 200.

## sgcp tse payload

To enable Inband Telephony Signaling Events (TSE) for fax and modem operation, use the **sgcp tse payload** command in global configuration mode. To restore the default value, use the **no** form of this command.

**sgcp tse payload** *type*

**no sgcp tse payload** *type*

<b>Syntax Description</b>	<i>type</i>	Sets the TSE payload type. The valid range is from 96 to 119. The default is 0, meaning that the command is disabled.
---------------------------	-------------	---

## show aal2 profile

To display the ATM adaptation layer 2 (AAL2) profiles configured on the system, use the **show aal2 profile** command in privileged EXEC mode.

**show aal2 profile all** | {**itut** *profile-number* | **custom** *profile-number* | **atmf** *profile-number*}

<b>Syntax Description</b>	<b>all</b>	Displays ATU-T, ATMF, and custom AAL2 profiles configured on the system.
	<b>itut</b>	Displays ATU-T profiles configured on the system.
	<i>profile-number</i>	Specifies the profile number of the AAL2 profile to display. The available choices are as follows:  For ITU-T: <ul style="list-style-type: none"> <li>• 1 = G.711ulaw</li> <li>• 2 = G.711ulaw with silence insertion descriptor (sid)</li> <li>• 7 = G.711ulaw and G.729ar8</li> </ul> For ATMF: None. ATMF is not supported.  For custom: <ul style="list-style-type: none"> <li>• 100 = G.711ulaw and G.726r32</li> <li>• 110 = G.711ulaw, G.726r32, and G.729ar8</li> </ul>
	<b>custom</b>	Displays custom profiles configured on the system.
	<b>atmf</b>	Displays ATMF profiles configured on the system.

## show atm video-voice address

To display the network service access point (NSAP) address for the ATM interface, enter the **show atm video-voice address** command in privileged EXEC mode.

```
show atm video-voice address
```

---

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

## show call active

To display active call information for voice calls or fax transmissions in progress, use the **show call active** command in user EXEC or privileged EXEC mode.

```
show call active {voice | fax}[brief]
```

---

<b>Syntax Description</b>	<b>voice</b>	Specifies that information be displayed for all active voice calls.
	<b>fax</b>	Specifies that information be displayed for all active fax calls.
	<b>brief</b>	(Optional) Displays a truncated version of the active call information.

---

## show call application voice

To define the names of the audio files that the interactive voice response (IVR) script will play, the operation of the abort keys, the prompts that are used, and caller interaction, use the **show call application voice** command in EXEC mode.

```
show call application voice [name | summary]
```

---

<b>Syntax Description</b>	<i>name</i>	(Optional) The name of the desired IVR application.
	<b>summary</b>	(Optional) Displays a one-line summary. If the command is entered without the <b>summary</b> keyword, a complete detailed description is displayed of the application.

---

## show call fallback cache

To see the current Calculated Planning Impairment Factor (ICPIF) estimates for all IP addresses in cache, use the **show call fallback cache** command in EXEC mode.

```
show call fallback cache [ip-address]
```

---

<b>Syntax Description</b>	<i>ip-address</i>	(Optional) Specifies a specific IP address.
---------------------------	-------------------	---

---

## show call fallback config

To display the call fallback configuration, use the **show call fallback config** command in EXEC mode.

```
show call fallback config
```

---

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

## show call fallback stats

To display the call fallback statistics, use the **show call fallback stats** command in EXEC mode.

```
show call fallback stats
```

---

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

## show call history

To display the call history table for voice calls or fax transmissions, use the **show call history** command in user EXEC or privileged EXEC mode.

```
show call history {voice | fax}[last number | brief]
```

---

<b>Syntax Description</b>	<b>voice</b>	Specifies that call history information be displayed for voice calls.
	<b>fax</b>	Specifies that call history information be displayed for fax calls.
	<b>last number</b>	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the <i>number</i> argument. Valid values are from 1 to 100.
	<b>brief</b>	(Optional) Displays a truncated version of the call history table.

---

## show call history video record

To display information about video calls, use the **show call history video record** command in privileged EXEC mode.

```
show call history video record
```

---

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

## show call history voice record

To display Call Detail Record (CDR) events in the call history table, use the **show call history voice record** command in privileged EXEC mode.

```
show call history voice record
```

---

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

## show call resource voice stats

To display resource statistics for an H.323 gateway, use the **show call resource voice stats** command in privileged EXEC mode.

```
show call resource voice stats
```

---

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

## show call resource voice threshold

To display the threshold configuration settings and status for an H.323 gateway, use the **show call resource voice threshold** command in privileged EXEC mode.

```
show call resource voice threshold
```

---

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

## show call rsvp-sync conf

To display the configuration settings for Resource Reservation Protocol (RSVP) synchronization, use the **show call rsvp-sync conf** command in privileged EXEC mode.

```
show call rsvp-sync conf
```

---

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

## show call rsvp-sync stats

To display statistics for calls that attempted Resource Reservation Protocol (RSVP) reservation, use the **show call rsvp-sync stats** command in privileged EXEC mode.

```
show call rsvp-sync stats
```

---

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

## show cdapi

To display the Call Distributor Application Programming Interface (CDAPI), use the **show cdapi** command in privileged EXEC mode.

```
show cdapi
```

---

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

## show ces clock-select

To display the setting of the network clock for the specified port, use the **show ces clock-select** command in privileged EXEC mode.

```
show ces slot/port clock-select
```

---

<b>Syntax Description</b>	<i>slot</i>	Backplane slot number.
	<i>lport</i>	Interface port number. The slash must be entered.

---

## show connect

To display configuration information about drop-and-insert connections that have been configured on a router, enter the **show connect** command in privileged EXEC mode.

```
show connect {all | elements | name | id | port {T1 | E1} slot/port}}
```

---

<b>Syntax Description</b>	<b>all</b>	Displays a table of all configured connections.
	<b>elements</b>	Displays registered hardware or software interworking elements.
	<b>name</b>	Displays a connection that has been named by using the <b>connect</b> global configuration command. The name you enter is case sensitive and must match the configured name exactly.

---

<b>id</b>	Displays the status of a connection that you specify by an identification number or range of identification numbers. The router assigns these IDs automatically in the order in which they were created, beginning with 1. The <b>show connect all</b> command displays these IDs.
<b>port</b>	Displays the status of a connection that you specify by indicating the type of controller (T1 or E1) and location of the interface.
<b>T1</b>	Specifies a T1 controller.
<b>E1</b>	Specifies an E1 controller.
<i>slot/port</i>	The location of the T1 or E1 controller port whose connection status you want to see. Valid values for <i>slot</i> and <i>port</i> are 0 and 1. The slash must be entered.

## show controllers timeslots

To show the channel-associated signaling (CAS) and ISDN PRI state in detail, use the **show controllers timeslots** command in privileged EXEC mode.

```
show controllers t1/e1 controller-number timeslots timeslot-range
```

Syntax Description		
	<b>t1/e1</b>	Specifies the type of interface.
	<i>controller-number</i>	Specifies the controller number of CAS or ISDN PRI time slot. Range 0 through 7.
	<b>timeslots</b>	Displays DS0 information.
	<i>timeslot-range</i>	Specifies time slot range 1 through 31 for E1, 1 through 24 for T1.

## show controllers rs366

To display information about the RS-366 video interface on the video dialing module (VDM), use the **show controllers rs366** command in privileged EXEC mode.

```
show controllers rs366 slot port
```

Syntax Description		
	<i>slot</i>	Slot location of the VDM module. On the Cisco MC3810 multiservice concentrator, this value is either 1 or 2. If you do not enter the correct location, the command is rejected.
	<i>port</i>	Port location of the EIA/TIA-366 interface in the VDM module. On the Cisco MC3810 multiservice concentrator, this value is 0.

## show controllers voice

To display information about voice-related hardware, use the **show controllers voice** command in privileged EXEC mode.

```
show controllers voice
```

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

## show csm

To display the call switching module (CSM) statistics for a particular digital signal processor (DSP) channel or all DSP channels or for a specific modem or DSP channel, use the **show csm** command in privileged EXEC mode.

### Cisco AS5300 Universal Access Server

```
show csm { modem [slot/port \ modem-group-number] | voice [slot/dspml/dspl/dsp-channel]}
```

### Cisco AS5800 Universal Access Server

```
show csm voice [shelf/slot/port]
```

<b>Syntax Description</b>	<b>modem</b>	Specifies CSM call statistics for modems.
	<b>voice</b>	Specifies CSM call statistics for DSP channels.
	<i>slot/port</i>	(Optional) Specifies the location (and thereby the identity) of a specific modem.
	<i>modem-group-number</i>	(Optional) Displays configuration for the dial peer identified by the argument <i>modem-group-number</i> . Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
	<i>slot/dspml/dspl/dsp-channel</i>	(Optional) Identifies the location of a particular DSP channel.
	<i>shelf/slot/port</i>	(Optional) Identifies the location of the voice interface card.

## show dial-peer video

To display dial-peer configuration, use the **show dial-peer video** command in privileged EXEC mode.

```
show dial-peer video [number] [summary]
```

<b>Syntax Description</b>	<i>number</i>	(Optional) A specific video dial peer. This option displays configuration information for a single dial peer identified by the argument <i>number</i> . Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
	<b>summary</b>	(Optional) Displays a summary of all video dial peer information.

## show dial-peer voice

To display configuration information for dial peers, use the **show dial-peer voice** command in privileged EXEC mode.

```
show dial-peer voice [number] [summary]
```

Syntax Description		
	<i>number</i>	(Optional) A specific dial peer. This option displays configuration information for a single dial peer identified by the <i>number</i> argument. Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
	<b>summary</b>	(Optional) Displays a summary of all voice dial peers.

## show dialplan incall number

To show which POTS dial peer is matched for a specific calling number or voice port, use the **show dialplan incall number** command in privileged EXEC mode.

```
show dialplan incall voice-port number calling-number
```

Syntax Description		
	<i>voice-port</i>	Specifies the voice port location. The syntax of this argument is platform-specific. For information on the syntax for a particular platform, see the <b>voice-port</b> global configuration command.
	<i>calling-number</i>	Specifies the calling number or ANI of the incoming voice call.

## show dialplan number

To show which dial peer is reached when a particular telephone number is dialed, use the **show dialplan number** command in privileged EXEC mode.

```
show dialplan number dial string
```

Syntax Description		
	<i>dial string</i>	Particular destination pattern (telephone number).

## show frame-relay vofr

To display information about the FRF.11 subchannels being used on Voice over Frame Relay (VoFR) data link controller identifiers (DLCIs), use the **show frame-relay vofr** command in privileged EXEC mode.

```
show frame-relay vofr [interface [dlci [cid]]]
```

## ■ show gatekeeper calls

<b>Syntax Description</b>	<i>interface</i>	(Optional) The specific interface type and number for which you wish to display FRF.11 subchannel information.
	<i>dlci</i>	(Optional) The specific data link connection identifier for which you wish to display FRF.11 subchannel information.
	<i>cid</i>	(Optional) The specific subchannel for which you wish to display information.

## show gatekeeper calls

To show the status of each ongoing call of which a gatekeeper is aware, use the **show gatekeeper calls** command in privileged EXEC mode.

**show gatekeeper calls**

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

## show gatekeeper endpoints

To display the status of all registered endpoints for a gatekeeper, use the **show gatekeeper endpoints** command in EXEC mode.

**show gatekeeper endpoints**

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

## show gatekeeper gw-type-prefix

To display the gateway technology prefix table, use the **show gatekeeper gw-type-prefix** command in privileged EXEC mode.

**show gatekeeper gw-type-prefix**

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

## show gatekeeper servers

To see a list of currently registered and statically configured triggers on this gatekeeper router, enter the **show gatekeeper servers** command in EXEC mode.

**show gatekeeper servers** [*gkid*]

**Syntax Description** *gkid* (Optional) The local gatekeeper name to which this trigger applies.

## show gatekeeper status

To show overall gatekeeper status, including authorization and authentication status, zone status, and so on, use the **show gatekeeper status** command in EXEC mode.

```
show gatekeeper status
```

---

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

## show gatekeeper zone prefix

To display the zone prefix table, use the **show gatekeeper zone prefix** command in privileged EXEC mode.

```
show gatekeeper zone prefix
```

---

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

## show gatekeeper zone status

To display the status of zones related to a gatekeeper, use the **show gatekeeper zone status** command in privileged EXEC mode.

```
show gatekeeper zone status
```

---

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

## show gateway

To display the current gateway status, use the **show gateway** command in privileged EXEC mode.

```
show gateway
```

---

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

## show interface dspfarm

To display digital signal processor (DSP) information on the two-port T1/E1 high-density port adapter for the Cisco 7200 series, use the **show interface dspfarm** command in privileged EXEC mode.

```
show interface dspfarm [slot/port] dsp [number] [long | short]
```

<b>Syntax Description</b>	<i>slot</i>	(Optional) Slot location of the port adapter.
	<i>/port</i>	(Optional) Port number on the port adapter.
	<b>dsp</b>	Specifies the DSP information.
	<i>number</i>	(Optional) Specifies the number of DSP sets to show. The range is 1 to 30.
	<b>long</b>	(Optional) Specifies detailed DSP information.
	<b>short</b>	(Optional) Specifies brief DSP information.

## show mgcp

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp** command in EXEC mode.

```
show mgcp [connection | endpoint | statistics]
```

<b>Syntax Description</b>	<b>connection</b>	(Optional) Displays the active MGCP-controlled connections.
	<b>endpoint</b>	(Optional) Displays the MGCP-controlled endpoints.
	<b>statistics</b>	(Optional) Displays MGCP statistics regarding network messages that have been received and sent.

## show num-exp

To show the number expansions configured, use the **show num-exp** command in privileged EXEC mode.

```
show num-exp [dialed-number]
```

<b>Syntax Description</b>	<i>dialed-number</i>	(Optional) Dialed number.
---------------------------	----------------------	---------------------------

## show pots csm

To show the current state of calls and the most recent event received by the call switching module (CSM) on the Cisco 800 series router, use the **show pots csm** command in EXEC mode.

```
show pots csm port
```

<b>Syntax Description</b>	<i>port</i>	Port number 1 or 2.
---------------------------	-------------	---------------------

## show pots status

To display the settings of the telephone port physical characteristics and other information on the telephone interfaces of the Cisco 800 series, use the **show pots status** command in privileged EXEC mode.

```
show pots status [1 | 2]
```

Syntax Description	1	(Optional) Display the settings of telephone port 1.
	2	(Optional) Display the settings of telephone port 2.

## show proxy h323 calls

To list each active call on the proxy, use the **show proxy h323 calls** command in privileged EXEC mode.

```
show proxy h323 calls
```

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

## show proxy h323 detail-call

To display the details of a particular call on a proxy, use the **show proxy h323 detail-call** command in privileged EXEC mode.

```
show proxy h323 detail-call call-key
```

Syntax Description	<i>call-key</i>	Specifies the call you want to display. The <i>call-key</i> argument is derived from the <b>show proxy h323 calls</b> display.
--------------------	-----------------	--

## show proxy h323 status

To display the overall status of a proxy, use the **show proxy h323 status** command in privileged EXEC mode.

```
show proxy h323 status
```

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

## show rawmsg

To show the raw messages owned by the required component, use the **show rawmsg** command in privileged EXEC mode.

```
show rawmsg {all | tsp | vtsp | ccapi | h323}
```

Syntax Description	all	All selections below.
	tsp	Telephony Service Provider subsystem.
	vtsp	Voice Telephony Service Provider subsystem.
	ccapi	API (Application Programming Interface) used to coordinate interaction between application and call legs (telephony or IP).
	h323	H.323 subsystem.

## show rtsp client session

To display cumulative information about Real Time Streaming Protocol (RTSP) session records, use the **show rtsp client session** command in privileged EXEC mode. To set the value to the default, use the **no** form of this command.

```
show rtsp client session {history | active} [detailed]
```

```
no show rtsp client session {history | active} [detailed]
```

Syntax Description	history	Displays cumulative information about the session, packet statistics, and general call information such as call ID, session ID, individual RTSP stream URLs, packet statistics, and play duration.
	active	If the keyword <b>detailed</b> is not specified, the command displays the session information and stream information for the stream that is currently active.
	detailed	(Optional) If the keyword <b>detailed</b> is specified, the command displays the session information and stream information in detail for all streams that are associated with the session.

## show settlement

To display the configuration for all settlement servers and see the specific provider and transactions, use the **show settlement** command in privileged EXEC mode. To reset to the default value, use the **no** form of this command.

```
show settlement [provider-number [transactions]]
```

```
no show settlement [provider-number [transactions]]
```

**Syntax Description**

<i>provider-number</i>	(Optional) Displays the attributes of a specific provider.
<b>transactions</b>	(Optional) Displays the transaction status of a specific provider.

## show sgcp connection

To see all active SGCP connections on this router, use the **show sgcp connection** command in EXEC mode.

```
show sgcp connection [interface number]
```

**Syntax Description**

<b>interface</b>	(Optional) Specifies a DS1 interface.
<i>number</i>	(Optional) Specifies the T1 interface (controller) number. Valid values on the Cisco MC3810 multiservice concentrator are from 0 to 1.

## show sgcp endpoint

To see SGCP endpoints eligible for SGCP management, use the **show sgcp endpoint** command in EXEC mode.

```
show sgcp endpoint [interface ds1 [ds0]]
```

**Syntax Description**

<b>interface <i>ds1</i></b>	(Optional) Specifies the DS1 interface for which to display SGCP endpoint information. The valid range is from 1 to 1000.
<i>ds0</i>	(Optional) Specifies the DS0 interface for which to display SGCP endpoint information. The valid range is from 0 to 30.

## show sgcp statistics

To see global statistics for the SGCP packet count, success and failure counts, and other information, use the **show sgcp statistics** command in EXEC mode.

```
show sgcp statistics
```

**Syntax Description**

This command has no arguments or keywords.

## show sip-ua

To display information and settings for the Session Initiation Protocol (SIP) User Agent (UA), use the **show sip-ua** command in privileged EXEC mode.

```
show sip-ua {retry | statistics | status | timers}
```

Syntax Description		
	<b>retry</b>	Displays SIP protocol retry counts.
	<b>statistics</b>	Displays SIP UA response, traffic, and retry statistics.
	<b>status</b>	Displays SIP UA listener status.
	<b>timers</b>	Displays current settings for the SIP UA protocol timers.

## show translation-rule

To display the contents of the rules that have been configured for a specific translation name, use the **show translation-rule** command in privileged EXEC mode.

```
show translation-rule [name-tag]
```

Syntax Description		
	<i>name-tag</i>	(Optional) The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. The range is from 1 through 2,147,483,647.

## show vfc

To see the entries in the host-name-and-address cache, use the **show vfc** command in privileged EXEC mode.

```
show vfc slot-number [technology]
```

Syntax Description		
	<i>slot-number</i>	VFC slot number.
	<b>technology</b>	(Optional) Displays the technology type of the VFC.

## show vfc cap-list

To show the current list of files on the capability list for this voice feature card (VFC), use the **show vfc cap-list** command in user EXEC mode.

```
show vfc slot cap-list
```

Syntax Description		
	<i>slot</i>	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.

## show vfc default-file

To show the default files included in the default file list for a voice feature card (VFC), use the **show vfc default-file** command in user EXEC mode.

```
show vfc slot default-file
```

<b>Syntax Description</b>	<i>slot</i>	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.
---------------------------	-------------	--

## show vfc directory

To show the list of all files residing on a voice feature card (VFC), use the **show vfc directory** command in user EXEC mode.

```
show vfc slot directory
```

<b>Syntax Description</b>	<i>slot</i>	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.
---------------------------	-------------	--

## show vfc version

To show the version of the software residing on a voice feature card (VFC), use the **show vfc version** command in user EXEC mode.

```
show vfc slot version {dspware | veware}
```

<b>Syntax Description</b>	<i>slot</i>	Identifies the slot where the VFC is installed. Valid values are 0, 1, and 2.
	<b>dspware</b>	Defines which DSPWare software to display.
	<b>veware</b>	Defines which VCWare software to display.

## show video call summary

To display summary information about video calls and the current status of the Video Call Manager (ViCM), use the **show video call summary** command in privileged EXEC mode.

```
show video call summary
```

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

## show voice busyout

To display information about the voice busyout state, use the **show voice busyout** command in privileged EXEC mode.

```
show voice busyout
```

---

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

## show voice call

To show the call status for voice ports on the Cisco router or concentrator, use the **show voice call** EXEC command.

### Cisco 2600 and 3600 series with Analog Voice Ports

```
show voice call [slot/subunit/port | summary]
```

### Cisco 2600 and 3600 Series with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)

```
show voice call [slot/port:ds0-group | summary]
```

### Cisco MC3810 Multiservice Concentrator with Analog Voice Ports

```
show voice call [slot/port | summary]
```

### Cisco MC3810 Multiservice Concentrator with Digital Voice Ports

```
show voice call [slot:ds0-group | summary]
```

---

**Syntax Description** For the Cisco 2600 and 3600 Series with Analog Voice Ports

<i>slot/subunit/port</i>	(Optional) Displays information for the analog voice port you specify with the <i>slot/subunit/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>subunit</i> specifies a voice interface card (VIC) where the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.)</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

**For the Cisco 2600 and 3600 Series with Digital Voice Ports**


---

<i>slot/port:ds0-group</i>	(Optional) Displays information for the digital voice port you specify with the <i>slot/port:ds0-group</i> designation. <ul style="list-style-type: none"> <li>• <i>slot</i> specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li>• <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.)</li> <li>• <i>ds0-group</i> specifies a T1 or E1 logical port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

---

**For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**


---

<i>slot/port</i>	(Optional) Displays information for the analog voice port you specify with the <i>slot/port</i> designation. <ul style="list-style-type: none"> <li>• <i>slot</i> is the physical slot in which the analog voice module (AVM) is installed. The <i>slot</i> is always 1 for analog voice ports in the Cisco MC3810 multiservice concentrator.</li> <li>• <i>port</i> specifies an analog voice port number. Valid entries are from 1 to 6.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

---

**For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**


---

<i>slot:ds0-group</i>	(Optional) Displays information for the digital voice port you specify with the <i>slot:ds0-group</i> designation. <ul style="list-style-type: none"> <li>• <i>slot</i> specifies the module (and controller). Valid entries are 0 for the MFT (controller 0) and 1 for the DVM (controller 1).</li> <li>• <i>ds0-group</i> specifies a T1 or E1 logical voice port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

---

## show voice dsp

To show the current status of all digital signal processor (DSP) voice channels, use the **show voice dsp** command in privileged EXEC mode.

**show voice dsp**

**Syntax Description**

This command has no arguments or keywords.

## show voice permanent-call

To display information about the permanent calls on a voice interface, use the **show voice permanent-call** command in user EXEC or privileged EXEC mode.

```
show voice permanent-call [voice-port] [summary]
```

---

### Syntax Description

<i>voice-port</i>	(Optional) Slot number or slot/port number of the voice interface for which you wish to display permanent call information.
<b>summary</b>	(Optional) Displays summary information about VoFR and VoATM ports used for permanent connections.

---

## show voice port

To display configuration information about a specific voice port, use the **show voice port** command in EXEC command.

### Cisco 1750 Router

```
show voice port slot-number/port
```

### Cisco 2600 and 3600 Series Router with Analog Voice Ports

```
show voice port [slot/subunit/port | summary]
```

### 2600 and 3600 Series Router with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)

```
show voice port [slot/port:ds0-group | summary]
```

### Cisco MC3810 Multiservice Concentrator with Analog Voice Ports

```
show voice port [slot/port | summary]
```

### Cisco MC3810 Multiservice Concentrator with Digital Voice Ports

```
show voice port [slot:ds0-group | summary]
```

### Cisco AS5300 Universal Access Server

```
show voice port controller number:D
```

### Cisco AS5800 Universal Access Server

```
show voice port {shelf/slot/port:D} | {shelf/slot/parent:port:D}
```

### Cisco 7200 Series Router

```
show voice port {slot/port:ds0-group-no} | {slot-number/subunit-number/port}
```

**Syntax Description****For the Cisco 1750 Router**

<i>slot-number</i>	Slot number in the router where the VIC is installed. Valid entries are from 0 to 2, depending on the slot where it has been installed.
<i>port</i>	Indicates the voice port. Valid entries are 0 or 1.

**For the Cisco 2600 and 3600 Series Router with Analog Voice Ports**

<i>slot/subunit/port</i>	(Optional) Displays information for the analog voice port you specify with the <i>slot/subunit/port</i> designation. <ul style="list-style-type: none"> <li>• <i>slot</i> specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li>• <i>subunit</i> specifies a voice interface card (VIC) where the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.)</li> <li>• <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

**For the Cisco 2600 and 3600 Series Router with Digital Voice Ports**

<i>slot/port:ds0-group</i>	(Optional) Displays information for the digital voice port you specify with the <i>slot/port:ds0-group</i> designation. <ul style="list-style-type: none"> <li>• <i>slot</i> specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li>• <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.)</li> <li>• <i>ds0-group</i> specifies a T1 or E1 logical port number. Valid entries are from 0 to 23 for T1 and from 0 to 30 for E1.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

**For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**

<i>slot/port</i>	(Optional) Displays information for the analog voice port you specify with the <i>slot/port</i> designation. <ul style="list-style-type: none"> <li>• <i>slot</i> is the physical slot in which the analog voice module (AVM) is installed. The <i>slot</i> is always 1 for analog voice ports in the Cisco MC3810 multiservice concentrator.</li> <li>• <i>port</i> specifies an analog voice port number. Valid entries are from 1 to 6.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

**For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**

<i>slot:ds0-group</i>	(Optional) Displays information for the digital voice port you specify with the <i>slot:ds0-group</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies the module (and controller). Valid entries are 0 for the MFT (controller 0) and 1 for the DVM (controller 1).</li> <li><i>ds0-group</i> specifies a T1 or E1 logical voice port number. Valid entries are from 0 to 23 for T1 and from 0 to 30 for E1.</li> </ul>
<b>summary</b>	(Optional) Displays a summary of all voice ports.

**For the Cisco AS5300 Access Server**

<i>controller number</i>	Specifies the T1 or E1 controller.
<b>:D</b>	Indicates the D channel associated with ISDN PRI.

**For the Cisco AS5800 Universal Access Server**

<i>shelf/slot/port</i>	Specifies the T1 or E1 controller on the T1 card. Valid entries for the <i>shelf</i> argument are from 0 to 9999. Valid entries for the <i>slot</i> argument are from 0 to 11. Valid entries for the <i>port</i> argument are from 0 to 11.
<i>shelf/slot/parent:port</i>	Specifies the T1 controller on the T3 card. Valid entries for the <i>shelf</i> argument are from 0 to 9999. Valid entries for the <i>slot</i> argument are from 0 to 11. Valid entries for the <i>port</i> argument is 1 to 28. The value for the <i>parent</i> argument is always 0.
<b>:D</b>	Indicates the D channel associated with ISDN PRI.

**For the Cisco 7200 Series Router**

<i>slot</i>	The router location where the voice port adapter is installed. Valid entries are from 0 to 3.
<i>port</i>	Indicates the voice interface card location. Valid entries are 0 and 1.
<i>dso-group-no</i>	Indicates the defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
<i>slot-number</i>	Indicates the slot number in the Cisco router where the voice interface card is installed. Valid entries are from 0 to 3, depending on the slot where it has been installed.
<i>subunit-number</i>	Indicates the subunit on the voice interface card where the voice port is located. Valid entries are 0 and 1.
<i>port</i>	Indicates the voice port number. Valid entries are 0 and 1.

## show voice trunk-conditioning signaling

To display the status of trunk-conditioning signaling and timing parameters for a voice port, use the **show voice trunk-conditioning signaling** command in user EXEC or privileged EXEC mode.

```
show voice trunk-conditioning signaling [summary | voice-port]
```

Syntax Description	summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
	<i>voice-port</i>	(Optional) Displays a detailed report for a specified voice port.

## show voice trunk-conditioning supervisory

To display the status of trunk supervision and configuration parameters for a voice port, use the **show voice trunk-conditioning supervisory** command in user EXEC or privileged EXEC mode.

```
show voice trunk-conditioning supervisory [summary | voice-port]
```

Syntax Description	summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
	<i>voice-port</i>	(Optional) Displays a detailed report for a specified voice port.

## show vrm active\_calls

To display active-only voice calls either for a specific voice feature card (VFC) or for all VFCs, use the **show vrm active\_calls** command in privileged EXEC mode.

```
show vrm active_calls {dial-shelf-slot-number | all}
```

Syntax Description	<i>dial-shelf-slot-number</i>	Slot number of the dial shelf. Valid number is 0 to 13.
	<b>all</b>	Lists all active calls for VFC slots.

## show vrm vdevices

To display detailed information for a specific digital signal processor (DSP) or a brief summary display for all voice feature cards (VFCs), use the **show vrm vdevices** command in privileged EXEC mode.

```
show vrm vdevices {{vfc-slot-number | voice-device-number} | summary}
```

**Syntax Description**

<i>vfc-slot-number</i>	Slot number of the VFC. Valid number is from 0 to 11.
<i>voice-device-number</i>	DSP number. Valid number is from 1 to 96.
<b>summary</b>	List synopsis of voice feature card DSP mappings, capabilities, and resource states.

## shut

To shut down a set of digital signal processors (DSPs) on the Cisco 7200 series router, use the **shut** command in DSP configuration mode. To put DSPs back in service, use the **no** form of this command.

**shut** *number*

**no shut** *number*

**Syntax Description**

<i>number</i>	Number of DSPs to be shut down.
---------------	---------------------------------

## shutdown

To change the administrative state of the selected dial peer from up to down, use the **shutdown** command in dial-peer configuration mode. To change the administrative state of this dial peer from down to up, use the **no** form of this command.

**shutdown**

**no shutdown**

**Syntax Description**

This command has no arguments or keywords.

## shutdown (DS1)

To shut down a DS1 link (send a Blue Alarm), use the **shutdown** command in controller configuration mode. To activate the DS1 (cancel the sending of the Blue Alarm), use the **no** form of the command.

**shutdown**

**no shutdown**

**Syntax Description**

This command has no arguments or keywords.

## shutdown (gatekeeper)

To disable the gatekeeper, use the **shutdown** command in gatekeeper configuration mode. To enable the gatekeeper, use the **no** form of this command.

**shutdown**

**no shutdown**

---

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

## shutdown (settlement)

To deactivate the settlement provider, use the **shutdown** command in settlement configuration mode. To activate a settlement provider, use the **no shutdown** command

**shutdown**

**no shutdown**

---

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

## shutdown (voice-port)

To take the voice ports for a specific voice interface card offline, use the **shutdown** command in voice-port configuration mode. To put the ports back in service, use the **no** form of this command.

**shutdown**

**no shutdown**

---

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





## Voice, Video, and Fax Commands: **signal** Through zone subnet

---

This chapter describes the function and syntax of the voice, video, and fax commands from **signal** through **zone subnet**. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Voice, Video, and Fax Command Reference*.

### signal

To specify the type of signaling for a voice port, use the **signal** command in voice-port configuration mode. To restore the default value for this command, use the **no** form of this command.

#### FXO and FXS Voice Ports

```
signal {loop-start | ground-start}
```

```
no signal {loop-start | ground-start}
```

#### E&M Voice Ports

```
signal {wink-start | immediate | delay-dial}
```

```
no signal {wink-start | immediate | delay-dial}
```

---

#### Syntax Description

<b>loop-start</b>	Specifies loop start signaling. Used for Foreign Exchange Office (FXO) and Foreign Exchange Station (FXS) interfaces. With loop start signaling only one side of a connection can hang up. This is the default setting for FXO and FXS voice ports.
<b>ground-start</b>	Specifies ground start signaling. Used for FXO and FXS interfaces. Ground start signalling allows both sides of a connection to place a call and to hang up.
<b>wink-start</b>	Indicates that the calling side seizes the line by going off-hook on its E-lead then waits for a short off-hook “wink” indication on its M-lead from the called side before sending address information as DTMF digits. Used for E&M tie trunk interfaces. This is the default setting for E&M voice ports.

---

<b>immediate</b>	Indicates that the calling side seizes the line by going off-hook on its E-lead and sends address information as DTMF digits. Used for E&M tie trunk interfaces.
<b>delay-dial</b>	Indicates that the calling side seizes the line by going off-hook on its E-lead. After a timing interval, the calling side looks at the supervision from the called side. If the supervision is on-hook, the calling side starts sending information as DTMF digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information. Used for E&M tie trunk interfaces.

## signal keepalive

To configure the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks, use the **signal keepalive** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

**signal keepalive** *number*

**no signal keepalive** *number*

<b>Syntax Description</b>	<i>number</i>	Specifies the keepalive signaling packet interval, in seconds. The valid range is from 1 to 65,535.
---------------------------	---------------	---

## signal pattern

To define the ABCD bit patterns that identify the idle and out-of-service (OOS) states for Cisco trunks and FRF.11 trunks, use the **signal pattern** command in voice-class configuration mode. To remove the signal pattern setting from the voice class, use the **no** form of this command.

**signal pattern** { **idle receive** | **idle transmit** | **oos receive** | **oos transmit** } *bit-pattern*

**no signal pattern** { **idle receive** | **idle transmit** | **oos receive** | **oos transmit** } *bit-pattern*

<b>Syntax Description</b>	<b>idle receive</b>	Defines the signaling pattern for identifying an idle message from the network. Also defines the idle signaling pattern to be sent to the PBX if the network trunk is out of service and the <b>signal sequence oos idle-only</b> or <b>signal sequence oos both</b> command is configured.
	<b>idle transmit</b>	Defines the signaling pattern for identifying an idle message from the PBX.
	<b>oos receive</b>	Defines the OOS signaling pattern to be sent to the PBX if the network trunk is out of service and the <b>signal sequence oos oos-only</b> or <b>signal sequence oos both</b> command is configured.
	<b>oos transmit</b>	Defines the signaling pattern for identifying an OOS message from the PBX.
	<i>bit-pattern</i>	Defines the ABCD bit pattern. Valid values are from 0000 to 1111.

## signal sequence oos

To specify which signaling pattern is sent to the PBX when the far-end keepalive message is lost or AIS is received from the far end, use the **signal sequence oos** command in the voice-class configuration mode. To restore the default value, use the **no** form of this command.

```
signal sequence oos { no-action | idle-only | oos-only | both }
```

```
no signal sequence oos
```

Syntax Description		
	<b>no-action</b>	No signaling pattern is sent.
	<b>idle-only</b>	Only the idle signaling pattern is sent.
	<b>oos-only</b>	Only the out-of-service (OOS) signaling pattern is sent.
	<b>both</b>	Both idle and OOS signaling patterns are sent. This is the default value.

## signal timing idle suppress-voice

To configure the signal timing parameter for the idle state of the call, use the **signal timing idle suppress-voice** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

```
signal timing idle suppress-voice seconds
```

```
no signal timing idle suppress-voice seconds
```

Syntax Description	<i>seconds</i>	
		Duration of the idle state, in seconds, before the voice traffic is stopped. The valid range is from 0 to 65,535.

## signal timing oos

To configure the signal timing parameter for the out-of-service (OOS) state of the call, use the **signal timing oos** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

```
signal timing oos { restart | slave-standby | suppress-all | suppress-voice | timeout } seconds
```

```
no signal timing oos { restart | slave-standby | suppress-all | suppress-voice | timeout } seconds
```

Syntax Description		
	<b>restart</b>	If no signaling packets are received for this period, the permanent voice connection will be torn down and an attempt to achieve reconnection will be made.
	<b>slave-standby</b>	If no signaling packets are received for this period, a slave port returns to its initial standby state. This option applies only to slave ports (ports configured using the <b>connection trunk number answer-mode</b> command).

<b>suppress-all</b>	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending all packets to the network.
<b>suppress-voice</b>	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending voice packets to the network. signaling packets continue to be sent with the alarm indication set (AIS).
<b>timeout</b>	If no signaling packets are received for this period of time, the router sends the configured receive OOS pattern to the PBX. Also, the router stops sending voice packets to the network. Use this option to perform busyout to the PBX.
<i>seconds</i>	Duration, in seconds, for the above settings. The valid range is from 0 to 65,535.

## signal timing oos restart

To specify that a permanent voice connection be torn down and restarted after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos restart** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

**signal timing oos restart** *seconds*

**no signal timing oos restart**

<b>Syntax Description</b>	<i>seconds</i>	Delay duration, in seconds, for the restart attempt. There is no default duration. The range is from 0 to 65,535.
---------------------------	----------------	---

## signal timing oos slave-standby

To configure a slave port to return to its initial standby state after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos slave-standby** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

**signal timing oos slave-standby** *seconds*

**no signal timing oos slave-standby**

<b>Syntax Description</b>	<i>seconds</i>	Delay duration, in seconds. If no signaling packets are received for this period, the slave port returns to its initial standby state. There is no default duration. The range is from 0 to 65,535.
---------------------------	----------------	---

## signal timing oos suppress-all

To configure the router or concentrator to stop sending voice and signaling packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-all** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

**signal timing oos suppress-all** *seconds*

**no signal timing oos suppress-all**

<b>Syntax Description</b>	<i>seconds</i>	Delay duration, in seconds, before packet transmission is stopped. There is no default duration. The range is from 0 to 65,535.
---------------------------	----------------	---

## signal timing oos suppress-voice

To configure the router or concentrator to stop sending voice packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-voice** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

**signal timing oos suppress-voice** *seconds*

**no signal timing oos suppress-voice**

<b>Syntax Description</b>	<i>seconds</i>	Delay duration, in seconds, before voice-packet transmission is stopped. There is no default duration. The range is from 0 to 65,535.
---------------------------	----------------	---

## signal timing oos timeout

To change the delay time between the loss of signaling packets from the network and the start time for the out-of-service (OOS) state, use the **signal timing oos timeout** command in voice-class configuration mode. To restore the default value, use the **no** form of this command.

**signal timing oos timeout** [*seconds* | **disabled**]

**no signal timing oos timeout**

<b>Syntax Description</b>	<i>seconds</i>	(Optional) Delay duration, in seconds, between the loss of signaling packets and the beginning of the OOS state. The default is 30 seconds. The range is from 1 to 65,535.
	<b>disabled</b>	(Optional) Deactivates the detection of packet loss. If no signaling packets are received from the network, the router does not send an OOS pattern to the PBX and it continues sending voice packets to the network. Use this option to disable busyout to the PBX.

## signal-type

To set the signaling type to be used when connecting to a dial peer, use the **signal-type** command in dial-peer configuration mode. To return to the default signal type, use the **no** form of this command.

**signal-type** { **cas** | **cept** | **ext-signal** | **transparent** }

**no signal-type**

Syntax Description	
<b>cas</b>	North American EIA-464 channel-associated signaling (robbed bit signaling). If the Digital T1 Packet Voice Trunk Network Module is installed, this option might not be available.
<b>cept</b>	Provides a basic E1 ABCD signaling protocol. Used primarily for E&M interfaces. When used with FXS/FXO interfaces, this protocol is equivalent to MELCAS.
<b>ext-signal</b>	External signaling. The DSP does not generate any signaling frames. Use this option when there is an external signaling channel, for example, CCS, or when you need to have a permanent “dumb” voice pipe.
<b>transparent</b>	On the Cisco MC3810 multiservice concentrator, selecting this option produces different results depending on whether you are using a digital voice module (DVM) or an analog voice module (AVM).  For a DVM: The ABCD signaling bits are copied from or transported through the T1/E1 interface “transparently” without modification or interpretation. This enables the Cisco MC3810 multiservice concentrator to handle arbitrary or unknown signaling protocols.  For an AVM: It is not possible to provide “transparent” behavior because the Cisco MC3810 must interpret the signaling information in order to read and write the correct state to the analog hardware. This option is mapped to be equal to <b>cas</b> .

## sip-server

To configure a network address for the Session Initiation Protocol (SIP) server interface, use the **sip-server** command in SIP user-agent configuration mode.

**sip-server** { **dns**:[*host-name*] | **ipv4**:*ip\_addr*[:*port-num*]}

Syntax Description	
<b>dns</b> :	Sets the global SIP server interface to a DNS host name. If you do not specify a host name, the default DNS defined by the <b>ip name-server</b> command is used.
<i>host-name</i>	(Optional) A valid DNS host name takes the following format: name.gateway.xyz.
<b>ipv4</b> : <i>ip_addr</i>	Sets the global SIP server interface to an IP address. A valid IP address takes the following format: xxx.xxx.xxx.xxx.
: <i>port-num</i>	(Optional) Specifies the port number for the SIP server.

## sip-ua

To enable the Session Initiation Protocol (SIP) user-agent configuration commands, with which you configure the user agent, use the **sip-ua** command in global configuration mode.

**sip-ua**

---

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

## snmp enable peer-trap poor-qov

To generate poor quality of voice notification for applicable calls associated with VoIP dial peers, use the **snmp enable peer-trap poor-qov** command in dial-peer configuration mode. To disable this notification, use the **no** form of this command.

**snmp enable peer-trap poor-qov**

**no snmp enable peer-trap poor-qov**

---

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

## station name

To specify the name that will be sent as caller ID information and to enable caller ID, use the **station name** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the name, use the **no** form of this command.

**station name** *name*

**no station name** *name*

---

**Syntax Description** *name* A string of 1 to 15 characters to represent the station name.

---

## station number

To specify the telephone or extension number that will be sent as caller ID information and to enable caller ID, use the **station number** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the number, use the **no** form of this command.

**station number** *number*

**no station number** *number*

---

<b>Syntax Description</b>	<i>number</i>	A string of 1 to 15 characters to represent the station number.
---------------------------	---------------	---

---

## subcell-mux

To enable subcell multiplexing on a Cisco MC3810 multiservice concentrator, use the **subcell-mux** command in voice-service configuration mode. To restore the default value, use the **no** form of the command.

**subcell-mux**

**no subcell-mux**

---

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

## supervisory disconnect

To enable a supervisory disconnect signal on Foreign Exchange Office (FXO) ports, use the **supervisory disconnect** command in voice-port configuration mode. To disable the supervisory disconnect signal, use the **no** form of this command.

**supervisory disconnect**

**no supervisory disconnect**

---

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

## supervisory disconnect anytone

To configure an Foreign Exchange Office (FXO) voice port to go on-hook if the router detects any tone from a PBX or PSTN before the call is answered, use the **supervisory disconnect anytone** command in voice-port configuration mode. To restore the default, use the **no** form of this command.

**supervisory disconnect anytone**

**no supervisory disconnect anytone**

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

## supervisory disconnect dualtone voice-class

To assign a previously configured voice class for Foreign Exchange Office (FXO) supervisory disconnect tone to a voice port, use the **supervisory disconnect dualtone voice-class** command in voice port configuration mode. To remove a voice class from a voice-port, use the **no** form of this command.

**supervisory disconnect dualtone** { **mid-call** | **pre-connect** } **voice-class** *tag*

**no supervisory disconnect dualtone voice-class** *tag*

<b>Syntax Description</b>	<b>mid-call</b>	Configures tone detection to operate throughout the duration of the call.
	<b>pre-connect</b>	Configures tone detection to operate during call setup and to stop when the called telephone goes off-hook.
	<i>tag</i>	A unique identification number assigned to one voice class. The tag number maps to the tag number assigned using the <b>voice class dualtone</b> global configuration command. The range is from 1 to 10,000.

## tdm-group

To configure a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect, use the **tdm-group** command in controller configuration mode. To delete a clear channel group, use the **no** form of this command.

**tdm-group** *tdm-group-no* **timeslot** *timeslot-list* [**type** { **e&m** | **fxs** [**loop-start** | **ground-start**] | **fxo** [**loop-start** | **ground-start**] | **fxs-melcas** | **fxo-melcas** | **e&m-melcas** }]

**no tdm-group** *tdm-group-no* **timeslot** *timeslot-list* [**type** { **e&m** | **fxs** [**loop-start** | **ground-start**] | **fxo** [**loop-start** | **ground-start**] | **fxs-melcas** | **fxo-melcas** | **e&m-melcas** }]

<b>Syntax Description</b>	<i>tdm-group-no</i>	TDM group number.
	<b>timeslot</b>	Time-slot number.

<i>timeslot-list</i>	Time-slot list. The valid range is from 1 to 24 for T1, and from 1 to 15 and 17 to 31 for E1.
<b>type</b>	<p>(Optional) (Valid only when the <b>mode cas</b> command is enabled.) Specifies the voice signaling type of the voice port. If configuring a TDM group for data traffic only, do not specify the type keyword.</p> <p>Choose from one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>e&amp;m</b>—for E&amp;M signaling</li> <li>• <b>fxs</b>—for Foreign Exchange Station signaling (optionally, you can also specify loop-start or ground-start)</li> <li>• <b>fxo</b>—for Foreign Exchange Office signaling (optionally, you can also specify loop-start or ground-start)</li> <li>• <b>fxs-melcas</b>—for Foreign Exchange Station MEL CAS</li> <li>• <b>fxo-melcas</b>—for Foreign Exchange Office MEL CAS</li> <li>• <b>e&amp;m-melcas</b>—for E&amp;M Mercury Exchange Limited Channel-Associated signaling (MEL CAS)</li> </ul> <p>The MELCAS options apply only to E1 lines and are used primarily in the United Kingdom.</p>

## tech-prefix

To specify that a particular technology prefix be prepended to the destination pattern of a specific dial peer, use the **tech-prefix** command in dial-peer configuration mode. To disable the defined technology prefix for this dial peer, use the **no** form of this command.

**tech-prefix** *number*

**no tech-prefix** *number*

### Syntax Description

<i>number</i>	Defines the numbers used as the technology prefix. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound (#) symbol is frequently used as the last character in a technology prefix. Valid characters are 0 through 9, the pound (#) symbol, and the asterisk (*).
---------------	---

## test call fallback probe

To test a probe to a particular IP address and display the Calculated Planning Impairment Factor (ICPIF) response time reporter (RTR) values, use the **test call fallback probe** command in EXEC mode. This command has no impact on the cache.

**test call fallback probe** *ip-address* [**codec** *711/729*]

### Syntax Description

<i>ip-address</i>	Specifies the target IP address.
<b>codec</b> <i>711/729</i>	(Optional) Specifies a specific codec type.

## test pots dial

To dial a telephone number for the POTS port on the router by using a dial application on your workstation, use the **test pots dial** command in EXEC mode.

```
test pots port dial number[#]
```

Syntax Description		
	<i>port</i>	Port number 1 or 2.
	<i>number</i>	Telephone number to dial.
	#	(Optional) Turns off dual tone multifrequency (DTMF) detection from the telephone while sending the <i>enbloc</i> signal. If you do not include the pound sign character (#) to terminate the <i>number</i> variable, you can use the telephone keypad to complete the call.

## test pots disconnect

To disconnect a telephone call for the POTS port on the router, use the **test pots disconnect** command in EXEC mode.

```
test pots port disconnect
```

Syntax Description		
	<i>port</i>	Port number 1 or 2.

## test translation-rule

To test the execution of the translation rules on a specific name tag, use the **test translation-rule** command in global configuration mode. To disable, use the **no** form of this command.

```
test translation-rule name-tag input-number [input-numbering-type]
```

```
no test translation-rule name-tag input-number [input-numbering-type]
```

Syntax Description		
	<i>name-tag</i>	The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. The range is 1 through 2,147,483,647.
	<i>input-number</i>	The input string of digits for which a pattern matching is performed.
	<i>input-numbering-type</i>	(Optional) The keyword choices for this field are <b>international</b> , <b>national</b> , <b>subscriber</b> , <b>abbreviated</b> , <b>unknown</b> , and <b>any</b> .

# test voice port detector

To test detector-related functions on a voice port, use the **test voice port detector** command in privileged EXEC mode.

## Cisco 2600 and 3600 Series with Analog Voice Ports

```
test voice port slot/subunit/port detector { m-lead | battery-reversal | ring | tip-ground |
ring-ground | ring-trip } { on | off | disable }
```

## Cisco 2600 and 3600 Series with Digital Voice Ports

```
test voice port slot/port:ds0-group detector { m-lead | battery-reversal | ring | tip-ground |
ring-ground | ring-trip } { on | off | disable }
```

## Cisco MC3810 Multiservice Concentrator with Analog Voice Ports

```
test voice port slot/port detector { m-lead | battery-reversal | ring | tip-ground | ring-ground |
ring-trip } { on | off | disable }
```

## Cisco MC3810 Multiservice Concentrator with Digital Voice Ports

```
test voice port slot:ds0-group detector { m-lead | battery-reversal | ring | tip-ground |
ring-ground | ring-trip } { on | off | disable }
```

### Syntax Description

#### For the Cisco 2600 and 3600 Series Routers with Analog Voice Ports

<i>slot/subunit/port</i>	Tests the voice port that you specify with the <i>slot/subunit/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1.</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.</li> </ul>
--------------------------	---

#### For the Cisco 2600 and 3600 Series Routers with Digital Voice Ports

<i>slot/port:ds0-group</i>	Tests the voice port that you specify with the <i>slot/port:ds0-group</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1.</li> <li><i>ds0-group</i> specifies a T1 or E1 logical port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
----------------------------	---

**For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**

<i>slot/port</i>	Tests the voice port that you specify with the <i>slot/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> is the physical slot in which the analog voice module (AVM) is installed. The <i>slot</i> is always 1 for analog voice ports in the Cisco MC3810.</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.</li> </ul>
------------------	--

**For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**

<i>slot:ds0-group</i>	Tests the voice port that you specify with the <i>slot:ds0-group</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies the module (and controller). Valid entries are 0 for the multiflex trunk module (MFT) (controller 0) and 1 for the DVM (controller 1).</li> <li><i>ds0-group</i> specifies a T1 or E1 logical voice port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
-----------------------	---

**For All Platforms**

<b>m-lead</b>	Forces the E&M m-lead detector to the specified state.
<b>loop</b>	Forces the FXO loop detector to the specified state.
<b>battery-reversal</b>	Forces the FXO battery-reversal detector to the specified state.
<b>ring</b>	Forces the FXO ringing detector to the specified state.
<b>tip-ground</b>	Forces the FXO tip-ground detector to the specified state.
<b>ring-ground</b>	Forces the FXS ring-ground detector to the specified state.
<b>ring-trip</b>	Forces the FXS ring-trip detector to the specified state.
<b>on</b>	Forces the selected item to the on state.
<b>off</b>	Forces the selected item to the off state.
<b>disable</b>	Ends the forced state for the selected item.

## test voice port inject-tone

To inject a test tone into a voice port, use the **test voice port inject-tone** command in privileged EXEC mode.

**Cisco 2600 and 3600 Series with Analog Voice Ports**

```
test voice port slot/subunit/port inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz
| 300hz | 3200hz | 3400hz | 500hz | quiet | disable}
```

**Cisco 2600 and 3600 Series with Digital Voice Ports**

```
test voice port slot/port:ds0-group inject-tone {local | network} {1000hz | 2000hz | 200hz |
3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet | disable}
```

**Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**

```
test voice port slot/port inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz
| 3200hz | 3400hz | 500hz | quiet | disable}
```

**Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**

```
test voice port slot:ds0-group inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz |
300hz | 3200hz | 3400hz | 500hz | quiet | disable}
```

**Syntax Description****For the Cisco 2600 and 3600 Series with Analog Voice Ports**

<i>slot/subunit/port</i>	Tests the voice port that you specify with the <i>slot/subunit/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1.</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.</li> </ul>
--------------------------	---

**For the Cisco 2600 and 3600 Series with Digital Voice Ports**

<i>slot/port:ds0-group</i>	Tests the voice port that you specify with the <i>slot/port:ds0-group</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1.</li> <li><i>ds0-group</i> specifies a T1 or E1 logical port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
----------------------------	---

**For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**

<i>slot/port</i>	Tests the voice port that you specify with the <i>slot/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> is the physical slot in which the analog voice module (AVM) is installed. The <i>slot</i> is always 1 for analog voice ports in the Cisco MC3810.</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.</li> </ul>
------------------	--

**For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**

<i>slot:ds0-group</i>	Tests the voice port that you specify with the <i>slot:ds0-group</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies the module (and controller). Valid entries are 0 for the multiflex trunk module (MFT) (controller 0) and 1 for the DVM (controller 1).</li> <li><i>ds0-group</i> specifies a T1 or E1 logical voice port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
-----------------------	---

**For All platforms**

<b>local</b>	Directs the injected tone toward the local interface (near end).
<b>network</b>	Directs the injected tone toward the network (far end).
<b>1000hz</b>	Injects a 1-kilohertz test tone.
<b>2000hz</b>	Injects a 2-kilohertz test tone.

<b>200hz</b>	Injects a 200-hertz test tone.
<b>3000hz</b>	Injects a 3-kilohertz test tone.
<b>300hz</b>	Injects a 300-hertz test tone.
<b>3200hz</b>	Injects a 3.2-kilohertz test tone.
<b>3400hz</b>	Injects a 3.4-kilohertz test tone.
<b>500hz</b>	Injects a 500-hertz test tone.
<b>quiet</b>	Injects a quiet tone.
<b>disable</b>	Ends the test tone.

## test voice port loopback

To perform loopback testing on a voice port, use the **test voice port loopback** command in privileged EXEC mode.

### Cisco 2600 and 3600 Series with Analog Voice Ports

```
test voice port slot/subunit/port loopback {local | network | disable}
```

### Cisco 2600 and 3600 Series with Digital Voice Ports

```
test voice port slot/port:ds0-group loopback {local | network | disable}
```

### Cisco MC3810 Multiservice Concentrator with Analog Voice Ports

```
test voice port slot/port loopback {local | network | disable}
```

### Cisco MC3810 Multiservice Concentrator with Digital Voice Ports

```
test voice port slot:ds0-group loopback {local | network | disable}
```

### Syntax Description

#### For the Cisco 2600 and 3600 Series with Analog Voice Ports

<i>slot/subunit/port</i>	Tests the voice port that you specify with the <i>slot/subunit/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1.</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.</li> </ul>
--------------------------	---

**For the Cisco 2600 and 3600 Series with Digital Voice Ports**


---

<i>slot/port:ds0-group</i>	Tests the voice port that you specify with the <i>slot/port:ds0-group</i> designation.
	<ul style="list-style-type: none"> <li>• <i>slot</i> specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li>• <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1.</li> <li>• <i>ds0-group</i> specifies a T1 or E1 logical port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>

---

**For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**


---

<i>slot/port</i>	Tests the voice port that you specify with the <i>slot/port</i> designation.
	<ul style="list-style-type: none"> <li>• <i>slot</i> is the physical slot in which the analog voice module (AVM) is installed. The <i>slot</i> is always 1 for analog voice ports in the Cisco MC3810.</li> <li>• <i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.</li> </ul>

---

**For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**


---

<i>slot:ds0-group</i>	Tests the voice port that you specify with the <i>slot:ds0-group</i> designation.
	<ul style="list-style-type: none"> <li>• <i>slot</i> specifies the module (and controller). Valid entries are 0 for the multiflex trunk module (MFT) (controller 0) and 1 for the DVM (controller 1).</li> <li>• <i>ds0-group</i> specifies a T1 or E1 logical voice port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>

---

**For All Platforms**


---

<b>local</b>	Forces a loopback at the voice port toward the customer premises equipment (CPE).
<b>network</b>	Forces a loopback at the voice port toward network.
<b>disable</b>	Ends the forced loopback.

---

## test voice port relay

To test relay-related functions on a voice port, use the **test voice port relay** command in privileged EXEC mode.

**Cisco 2600 and 3600 Series with Analog Voice Ports**

```
test voice port slot/subunit/port relay {e-lead | loop | ring-ground | battery-reversal |
power-denial | ring | tip-ground} {on | off | disable}
```

**Cisco 2600 and 3600 Series with Digital Voice Ports**

```
test voice port slot/port:ds0-group relay {e-lead | loop | ring-ground | battery-reversal |
power-denial | ring | tip-ground} {on | off | disable}
```

**Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**

```
test voice port slot/port relay {e-lead | loop | ring-ground | battery-reversal | power-denial |
ring | tip-ground} {on | off | disable}
```

**Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**

```
test voice port slot:ds0-group relay {e-lead | loop | ring-ground | battery-reversal |
power-denial | ring | tip-ground} {on | off | disable}
```

**Syntax Description****For the Cisco 2600 and 3600 Series with Analog Voice Ports**


---

<i>slot/subunit/port</i>	Tests the voice port that you specify with the <i>slot/subunit/port</i> designation.
	<ul style="list-style-type: none"> <li>• <i>slot</i> specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li>• <i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1.</li> <li>• <i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.</li> </ul>

---

**For the Cisco 2600 and 3600 Series with Digital Voice Ports**


---

<i>slot/port:ds0-group</i>	Tests the voice port that you specify with the <i>slot/port:ds0-group</i> designation.
	<ul style="list-style-type: none"> <li>• <i>slot</i> specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li>• <i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1.</li> <li>• <i>ds0-group</i> specifies a T1 or E1 logical port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>

---

**For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**


---

<i>slot/port</i>	Tests the voice port that you specify with the <i>slot/port</i> designation.
	<ul style="list-style-type: none"> <li>• <i>slot</i> is the physical slot in which the analog voice module (AVM) is installed. The <i>slot</i> is always 1 for analog voice ports in the Cisco MC3810.</li> <li>• <i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.</li> </ul>

---

**For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**


---

<i>slot:ds0-group</i>	Tests the voice port that you specify with the <i>slot:ds0-group</i> designation.
	<ul style="list-style-type: none"> <li>• <i>slot</i> specifies the module (and controller). Valid entries are 0 for the multiflex trunk module (MFT) (controller 0) and 1 for the DVM (controller 1).</li> <li>• <i>ds0-group</i> specifies a T1 or E1 logical voice port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>

---

**For All Platforms:**

<b>e-lead</b>	Forces the E&M e-lead relay to the specified state.
<b>loop</b>	Forces the FXO loop relay to the specified state.
<b>ring-ground</b>	Forces the FXO ring-ground relay to the specified state.
<b>battery-reversal</b>	Forces the FXO battery-reversal relay to the specified state.
<b>power-denial</b>	Forces the FXS power-denial relay to the specified state.
<b>ring</b>	Forces the FXS ringing relay to the specified state.
<b>tip-ground</b>	Forces the FXS tip-ground relay to the specified state.
<b>on</b>	Forces the selected item to the on state.
<b>off</b>	Forces the selected item to the off state.
<b>disable</b>	Ends the forced state for the selected item.

## test voice port switch

To force a voice port into fax mode, use the **test voice port switch** command in privileged EXEC mode.

### Cisco 2600 and 3600 Series with Analog Voice Ports

```
test voice port slot/subunit/port switch {fax | disable}
```

### Cisco 2600 and 3600 Series with Digital Voice Ports

```
test voice port slot/port:ds0-group switch {fax | disable}
```

### Cisco MC3810 Multiservice Concentrator with Analog Voice Ports

```
test voice port slot/port switch {fax | disable}
```

### Cisco MC3810 Multiservice Concentrator with Digital Voice Ports

```
test voice port slot:ds0-group switch {fax | disable}
```

### Syntax Description

#### For the Cisco 2600 and 3600 Series with Analog Voice Ports

<i>slot/subunit/port</i>	Tests the voice port that you specify with the <i>slot/subunit/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>subunit</i> specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1.</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 0 and 1.</li> </ul>
--------------------------	---

**For the Cisco 2600 and 3600 Series with Digital Voice Ports**


---

<i>slot/port:ds0-group</i>	Tests the voice port that you specify with the <i>slot/port:ds0-group</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform.</li> <li><i>port</i> specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1.</li> <li><i>ds0-group</i> specifies a T1 or E1 logical port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
----------------------------	---

---

**For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports**


---

<i>slot/port</i>	Tests the voice port that you specify with the <i>slot/port</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> is the physical slot in which the analog voice module (AVM) is installed. The <i>slot</i> is always 1 for analog voice ports in the Cisco MC3810.</li> <li><i>port</i> specifies an analog voice port number. Valid entries are 1 to 6.</li> </ul>
------------------	--

---

**For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports**


---

<i>slot:ds0-group</i>	Tests the voice port that you specify with the <i>slot:ds0-group</i> designation. <ul style="list-style-type: none"> <li><i>slot</i> specifies the module (and controller). Valid entries are 0 for the multiflex trunk module (MFT) (controller 0) and 1 for the DVM (controller 1).</li> <li><i>ds0-group</i> specifies a T1 or E1 logical voice port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.</li> </ul>
-----------------------	---

---

**For All Platforms**


---

<b>fax</b>	Forces a switch to fax mode.
<b>disable</b>	Ends fax mode; switches back to voice mode.

---

## test vrm busyout

To busy out a specific digital signal processor (DSP) or channels on a specific DSP, use the **test vrm busyout** command in privileged EXEC mode.

```
test vrm busyout slot-number {first-dsp-number {last-dsp-number | channel number} | all}
```

**Syntax Description**


---

<i>slot-number</i>	Number that identifies the slot in which the VFC is installed. Values for this argument are 0 to 11.
<i>first-dsp-number</i>	Specifies the first DSP in a range to be busied out. Each VFC holds 96 DSPs, so the value for this argument is 1 to 96.
<i>last-dsp-number</i>	Specifies the last DSP in a range to be busied out. Each VFC holds 96 DSPs, so the value for this argument is 1 to 96.
<b>channel</b>	Specifies that a certain channel on the specified DSPs will be busied out.

---

<i>number</i>	Indicates the channel to be busied out. Values are 1 or 2.
<b>all</b>	Indicates that all 96 DSPs on the VFC installed in the defined slot will be busied out.

## test vrm reset

To reset a particular digital signal processor (DSP), use the **test vrm reset** command in privileged EXEC mode.

```
test vrm reset slot-number dsp-number
```

### Syntax Description

<i>slot-number</i>	Number that identifies the slot in which the VFC is installed.
<i>dsp-number</i>	Number that identifies the DSP to be reset.

## test vrm unbusyout

To restore activity to a busied-out digital signal processor (DSP) or busied-out channels on a DSP, use the **test vrm unbusyout** command in privileged EXEC mode.

```
test vrm unbusyout slot-number {first-dsp-number {last-dsp-number | channel number} | all }
```

### Syntax Description

<i>slot-number</i>	Number that identifies the slot in which the VFC is installed. Values for this field are 0 to 11.
<i>first-dsp-number</i>	Specifies the first DSP in a range to be restored. Each VFC holds 96 DSPs, so the value for this argument is 1 to 96.
<i>last-dsp-number</i>	Specifies the last DSP in a range to be restored. Each VFC holds 96 DSPs, so the value for this argument is 1 to 96.
<b>channel</b>	Specifies that a certain channel on the specified DSPs will be restored.
<i>number</i>	Indicates the channel to be restored. Values are 1 or 2.
<b>all</b>	Indicates that all 96 DSPs on the VFC installed in the defined slot will be restored.

## timeouts call-disconnect

To configure the call disconnect timeout value for a specified voice port, use the **timeouts call-disconnect** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

```
timeouts call-disconnect seconds
```

```
no timeouts call-disconnect
```

### Syntax Description

<i>seconds</i>	Sets the call-disconnect timeout duration, in seconds. Valid values are from 0 to 120.
----------------	--

## timeouts initial

To configure the initial digit timeout value for a specified voice port, use the **timeouts initial** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**timeouts initial** *seconds*

**no timeouts initial** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Initial timeout duration, in seconds. Valid entries are any integer from 0 to 120.
---------------------------	----------------	--

## timeouts interdigit

To configure the interdigit timeout value for a specified voice port, use the **timeouts interdigit** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**timeouts interdigit** *seconds*

**no timeouts interdigit** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Interdigit timeout duration, in seconds. Valid entries are any integer from 0 to 120.
---------------------------	----------------	---

## timeouts ringing

To configure the timeout value for ringing, use the **timeouts ringing** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**timeouts ringing** {*seconds* | **infinity**}

**no timeouts ringing**

<b>Syntax Description</b>	<i>seconds</i>	The duration, in seconds, for which a voice port allows ringing to continue if a call is not answered. The range is from 5 to 60,000. The default is 180.
	<b>infinity</b>	Ringing continues until the caller goes on-hook.

## timeouts wait-release

To configure the delay timeout before the system starts the process for releasing voice ports, use the **timeouts wait-release** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**timeouts wait-release** { *seconds* | **infinity** }

**no timeouts wait-release**

Syntax Description	<i>seconds</i>	The duration, in seconds, for which a voice port stays in the call-failure state while the Cisco router or concentrator sends a busy tone, reorder tone, or out-of-service tone to the port. The range is from 3 to 3600. The default is 30.
	<b>infinity</b>	The voice port is never released as long as the call-failure state remains.

## timers

To configure the SIP signaling timers, use the **timers** command in the session initiation protocol (SIP) user agent configuration mode. To restore the default value, use the **no** form of this command.

**timers** { **trying** *number* | **connect** *number* | **disconnect** *number* | **expires** *number* }

**no timers** { **trying** *number* | **connect** *number* | **disconnect** *number* | **expires** *number* }

<b>Syntax Description</b>	<b>trying</b> <i>number</i>	Time (in milliseconds) to wait for a 100 response to an INVITE request. Possible values are 100 through 1000. The default is 500.
	<b>connect</b> <i>number</i>	Time (in milliseconds) to wait for a 200 response to an ACK request. Possible values are 100 through 1000. The default is 500.
	<b>disconnect</b> <i>number</i>	Time (in milliseconds) to wait for a 200 response to a BYE request. Possible values are 100 through 1000. The default is 500.
	<b>expires</b> <i>number</i>	Time (in milliseconds) for which an INVITE request is valid. Possible values are 60000 through 300,000. The default is 180,000.

## timing clear-wait

To indicate the minimum amount of time between the inactive seizure signal and the call being cleared for a specified voice port, use the **timing clear-wait** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing clear-wait** *milliseconds*

**no timing clear-wait** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Minimum amount of time, in milliseconds, between the inactive seizure signal and the call being cleared. Valid entries on the Cisco 3600 series are numbers from 200 to 2000. Valid entries on the Cisco MC3810 are numbers from 100 to 2000. Supported on E&M ports only.
---------------------------	---------------------	--

## timing delay-duration

To specify the delay signal duration for a specified voice port, use the **timing delay-duration** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing delay-duration** *milliseconds*

**no timing delay-duration** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Delay signal duration for delay dial signaling, in milliseconds. Valid entries are numbers from 100 to 5000. Supported on E&M ports only.
---------------------------	---------------------	---

## timing delay-start

To specify the minimum delay time from outgoing seizure to ou-dial address for a specified voice port, use the **timing delay-start** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing delay-start** *milliseconds*

**no timing delay-start** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Minimum delay time, in milliseconds, from outgoing seizure to outdial address. Valid entries are numbers from 20 to 2000. Supported on E&M ports only.
---------------------------	---------------------	--

## timing delay-with-integrity

To specify the duration of the wink pulse for the delay dial for a specified voice port on the Cisco MC3810, use the **timing delay-with-integrity** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing delay-with-integrity** *milliseconds*

**no timing delay-with-integrity** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Duration of the wink pulse for the delay dial, in milliseconds. Valid entries are numbers from 0 to 5000. Supported on E&M ports only.
---------------------------	---------------------	--

## timing dial-pulse min-delay

To specify the time between wink-like pulses for a specified voice port, use the **timing dial-pulse min-delay** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing dial-pulse min-delay** *milliseconds*

**no timing dial-pulse min-delay** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Time, in milliseconds, between the generation of wink-like pulses. Valid entries are integers from 0 to 5000.
---------------------------	---------------------	---

## timing dialout-delay

To specify the dial-out delay for the sending digit on a specified voice port on the Cisco MC3810 multiservice concentrator, use the **timing dialout-delay** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing dialout-delay** *milliseconds*

**no timing dialout-delay** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	Dial-out delay, in milliseconds, for the sending digit or cut-through on an FXO trunk or an E&M immediate trunk. Valid entries are from 100 to 5000 milliseconds.
---------------------------	---------------------	---

## timing digit

To specify the DTMF digit signal duration for a specified voice port, use the **timing digit** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing digit** *milliseconds*

**no timing digit** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	The DTMF digit signal duration, in milliseconds. Valid entries are integers from 50 to 100. Supported on FXO, FXS and E&M ports.
---------------------------	---------------------	--

## timing guard-out

To specify the guard-out duration of an Foreign Exchange Office (FXO) voice port, use the **timing guard-out** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**timing guard-out** *milliseconds*

**no timing guard-out**

<b>Syntax Description</b>	<i>milliseconds</i>	Duration, in milliseconds, of the guard-out period. The range is 300 to 3000. The default is 2000.
---------------------------	---------------------	--

## timing hookflash-input

To specify the maximum duration of a hookflash for an Foreign Exchange Station (FXS) interface, use the **timing hookflash-input** command in privileged EXEC mode. To restore the default duration for hookflash timing, use the **no** form of this command.

**timing hookflash-input** *milliseconds*

**no timing hookflash-input**

<b>Syntax Description</b>	<i>milliseconds</i>	Duration of the hookflash, in milliseconds. Possible values are 50 through 1550 milliseconds.
---------------------------	---------------------	---

## timing hookflash-output

To specify the duration of hookflash indications that the gateway generates on a Foreign Exchange Office (FXO) interface, use the **timing hookflash-output** command in voice-port configuration mode. To restore the default duration for hookflash timing, use the **no** form of this command.

**timing hookflash-output** *milliseconds*

**no timing hookflash-output**

<b>Syntax Description</b>	<i>milliseconds</i>	Duration of the hookflash, in milliseconds. Possible values are 50 through 1550 milliseconds.
---------------------------	---------------------	---

## timing interdigit

To specify the dual-tone multifrequency (DTMF) interdigit duration for a specified voice port, use the **timing interdigit** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing interdigit** *milliseconds*

**no timing interdigit** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	DTMF interdigit duration, in milliseconds. Valid entries are numbers from 50 to 500 milliseconds. Supported on FXO, FXS and E&M ports.
---------------------------	---------------------	--

## timing percentbreak

To specify the percentage of the break period for dialing pulses for a voice port, use the **timing percentbreak** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing percentbreak** *percent*

**no timing percentbreak**

<b>Syntax Description</b>	<i>percent</i>	Percentage of the break period for dialing pulses. Valid entries are from 20 to 80. The default is 50.
---------------------------	----------------	--

## timing pulse

To specify the pulse dialing rate for a specified voice port, use the **timing pulse** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing pulse** *pulses-per-second*

**no timing pulse** *pulses-per-second*

<b>Syntax Description</b>	<i>pulses-per-second</i>	Pulse dialing rate, in pulses per second. Valid entries are numbers from 10 to 20. Supported on FXO and E&M ports only.
---------------------------	--------------------------	---

## timing pulse-interdigit

To specify the pulse interdigit timing for a specified voice port, use the **timing pulse-interdigit** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing pulse-interdigit** *milliseconds*

**no timing pulse-interdigit** *milliseconds*

---

**Syntax Description***milliseconds*

Pulse dialing interdigit timing, in milliseconds. Valid entries are integers from 100 to 1000. Supported on FXO and E&M ports only.

---

## timing wink-duration

To specify the maximum wink-signal duration for a specified voice port, use the **timing wink-duration** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

**timing wink-duration** *milliseconds*

**no timing wink-duration** *milliseconds*

---

**Syntax Description***milliseconds*

Maximum wink-signal duration, in milliseconds, for a wink-start signal. Valid entries are from 100 to 400 milliseconds. Supported on E&M ports only.

---

## timing wink-wait

To specify the maximum wink-wait duration for a specified voice port, use the **timing wink-wait** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**timing wink-wait** *milliseconds*

**no timing wink-wait** *milliseconds*

---

**Syntax Description***milliseconds*

Maximum wink-wait duration, in milliseconds, for a wink start signal. Valid entries are from 100 to 5000 milliseconds. Supported on E&M ports only.

---

## token-root-name

To specify which root or Certificate Authority (CA) certificate the router should use to validate the settlement token in the incoming setup message, use the **token-root-name** command in settlement configuration mode. To restore the default value, use the **no** form of this command.

**token-root-name** *name*

**no token-root-name** *name*

### Syntax Description

<i>name</i>	Specifies the name that is the certificate identification as configured through the <b>crypto ca identity</b> <i>name</i> command or the <b>crypto ca trusted-root</b> <i>name</i> command.
-------------	---

## translate

To apply a translation rule to an inbound plain old telephone service (POTS) call leg, use the **translate** command in voice-port configuration mode. To remove the translation rule to an inbound POTS call leg, use the **no** form of this command.

**translate** { **calling-number** | **called-number** } *name-tag*

**no translate** { **calling-number** | **called-number** } *name-tag*

### Syntax Description

<b>calling-number</b>	Applies the translation rule to the inbound calling party number.
<b>called-number</b>	Applies the translation rule to the inbound called party number.
<i>name-tag</i>	The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. The range is 1 through 2,147,483,647.

## translate-outgoing

To apply a translation rule to an outbound plain old telephone service (POTS) or Voice over IP (VoIP) call leg, use the **translate-outgoing** command in dial-peer configuration mode. To remove the translation rule to an outbound POTS or VoIP call leg, use the **no** form of this command.

**translate-outgoing** { **calling-number** | **called-number** } *name-tag*

**no translate-outgoing** { **calling-number** | **called-number** } *name-tag*

### Syntax Description

<b>calling-number</b>	Applies the translation rule to the outbound calling party number.
<b>called-number</b>	Applies the translation rule to the outbound called party number.
<i>name-tag</i>	The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. The range is 1 through 2,147,483,647.

## translation-rule

To create a translation name and enter translation-rule configuration mode to apply rules to the translation name, use the **translation-rule** command in global configuration mode. To remove the translation rule, use the **no** form of this command.

**translation-rule** *name-tag*

**no translation-rule** *name-tag*

### Syntax Description

<i>name-tag</i>	The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. The range is 1 through 2,147,483,647.
-----------------	--

## transport

To configure the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket, use the **transport** command in SIP user-agent configuration mode. To block reception of SIP signaling messages on a particular socket, use the **no** form of this command.

**transport** {**udp** | **tcp**}

**no transport** {**udp** | **tcp**}

### Syntax Description

<b>udp</b>	Configures the SIP user agent to receive SIP messages on UDP port 5060.
<b>tcp</b>	Configures the SIP user agent to receive SIP messages on TCP port 5060.

## type (voice)

To specify the E&M interface type, use the **type** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

**type** {**1** | **2** | **3** | **5**}

**no type** {**1** | **2** | **3** | **5**}

### Syntax Description

<b>1</b>	Indicates the following lead configuration: <ul style="list-style-type: none"> <li>E—Output, relay to ground.</li> <li>M—Input, referenced to ground.</li> </ul>
<b>2</b>	Indicates the following lead configuration: <ul style="list-style-type: none"> <li>E—Output, relay to SG.</li> <li>M—Input, referenced to ground.</li> <li>SB—Feed for M, connected to –48V.</li> <li>SG—Return for E, galvanically isolated from ground.</li> </ul>

3	Indicates the following lead configuration: <ul style="list-style-type: none"> <li>• E—Output, relay to ground.</li> <li>• M—Input, referenced to ground.</li> <li>• SB—Connected to -48V.</li> <li>• SG—Connected to ground.</li> </ul>
5	Indicates the following lead configuration: <ul style="list-style-type: none"> <li>• E—Output, relay to ground.</li> <li>• M—Input, referenced to -48V.</li> </ul>

## type (settlement)

To point to the provider type and the specific settlement server, use the **type** command in settlement configuration mode. To disable this command, use the **no** form of this command.

**type** {osp | uni-osp}

**no type**

Syntax Description	
<b>osp</b>	Enables the Open Settlement Protocol (OSP) server type.
<b>uni-osp</b>	Enables authentication of Voice over IP (VoIP) calls to the Public Switched Telephone Network (PSTN) using a single settlement server.

## unbundle vfc

To unbundle DSPWare from the VCWare and configure the default file and capability lists with default values, use the **unbundle vfc** command in privileged EXEC mode.

**unbundle** [high-complexity | medium-complexity] vfc *slot-number*

Syntax Description	
<b>high-complexity</b>	(Optional) Unbundles the high-complexity firmware set.
<b>medium-complexity</b>	(Optional) Unbundles the medium-complexity firmware set.
<i>slot-number</i>	Indicates the VFC slot number.

## url

To configure the Internet service provider (ISP) address, use the **url** command in settlement configuration mode. To disable this command, use the **no** form of this command.

**url** *url-address*

**no url** *url-address*

**Syntax Description**

<i>url-address</i>	A valid URL address is: <code>http://fully qualified domain name[:port]/[URL]</code>
--------------------	---

## use-proxy

To enable proxy communications for calls between local and remote zones, use the **use-proxy** command in gatekeeper configuration mode. To either remove a proxy configuration entry for a remote zone or disable proxy communications between local and remote zones, use the **no** form of this command.

```
use-proxy local-zone-name {default | remote-zone remote-zone-name} {inbound-to | outbound-from} {gateway | terminal}
```

```
no use-proxy local-zone-name remote-zone remote-zone-name [{inbound-to | outbound-from} {gateway | terminal}]
```

**Syntax Description**

<i>local-zone-name</i>	The name or zone name of the gatekeeper, which is usually the fully domain-qualified host name of the gatekeeper. For example, if the domain name is cisco.com, the gatekeeper name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the name of the gatekeeper for each zone should be a unique string that has a mnemonic value.
<b>default</b>	Defines the default proxy policy for all calls that are not defined by a <b>use-proxy</b> command with the <b>remote-zone</b> keyword.
<b>remote-zone</b> <i>remote-zone-name</i>	Defines a proxy policy for calls to or from a specific remote gatekeeper or zone.
<b>inbound-to</b>	Applies the proxy policy to calls that are inbound to the local zone from a remote zone. Each <b>use-proxy</b> command defines the policy for only one direction.
<b>outbound-from</b>	Applies the proxy policy to calls that are outbound from the local zone to a remote zone. Each <b>use-proxy</b> command defines the policy for only one direction.
<b>gateway</b>	Defines the type of local device to which the policy applies. The <b>gateway</b> option applies the policy only to local gateways.
<b>terminal</b>	Defines the type of local device to which the policy applies. The <b>terminal</b> option applies the policy only to local terminals.

## vad (dial peer)

To enable voice activity detection (VAD) for the calls using this dial peer, use the **vad** command in dial-peer configuration mode. To disable VAD, use the **no** form of this command.

```
vad
```

```
no vad
```

**Syntax Description**

This command has no arguments or keywords.

## vad (voice-port)

To enable voice activity detection (VAD) for the calls using this voice port, use the **vad** command in voice-port configuration mode. To disable VAD, use the **no** form of this command.

**vad**

**no vad**

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

## vbr-rt

To configure the real-time variable bit rate (VBR) for Voice over ATM connections, use the **vbr-rt** command in ATM virtual circuit configuration mode. To restore the default, use the **no** form of this command.

**vbr-rt** *peak-rate average-rate burst*

**no vbr-rt**

Syntax Description		
<i>peak-rate</i>		The peak information rate (PIR) of the voice connection, in kbps. The range is 56 to 10,000.
<i>average-rate</i>		The average information rate (AIR) of the voice connection, in kbps. The range is 1 to 56.
<i>burst</i>		Burst size, in number of cells. The range is 0 to 65,536.

## vofr

To enable Voice over Frame Relay (VoFR) on a specific data-link connection identifier (DLCI) and to configure specific subchannels on that DLCI, use the **vofr** command in frame relay DLCI configuration mode. To disable VoFR on a specific DLCI, use the **no** form of this command.

### Switched Calls

**vofr** [*data cid*] [*call-control [cid]*]

**no vofr** [*data cid*] [*call-control [cid]*]

### Switched Calls to Cisco MC3810 Multiservice Concentrators Running Cisco IOS Releases Before 12.0(7)XK and 12.1(2)T

**vofr** [*cisco*]

**no vofr** [*cisco*]

**Cisco-Trunk Permanent Calls**

**vofr data *cid* call-control *cid***

**no vofr data *cid* call-control *cid***

**Cisco-Trunk Permanent Calls to Cisco MC3810 Multiservice Concentrators Running Cisco IOS Releases Before 12.0(7)XK and 12.1(2)T**

**vofr cisco**

**no vofr cisco**

**FRF-11 Trunk Calls**

**vofr [*data cid*] [*call-control cid*]**

**no vofr [*data cid*] [*call-control cid*]**

Syntax Description		
<b>data</b>	(Required for Cisco-trunk permanent calls. Optional for switched calls.) Used to select a subchannel (CID) for data other than the default subchannel, which is 4.	
<i>cid</i>	(Optional) Specifies the subchannel to be used for data. Valid values are from 4 through 255; the default is 4. If <b>data</b> is specified, enter a valid CID.	
<b>call-control</b>	(Optional) Used to specify that a subchannel will be reserved for call-control signaling. This option is not supported on the Cisco MC3810 multiservice concentrator.	
<b>cisco</b>	(Optional) Cisco proprietary voice encapsulation for VoFR with data is carried on CID 4 and call-control on CID 5. This option is required when configuring switched calls or Cisco trunks to Cisco MC3810 multiservice concentrators running Cisco IOS Releases before 12.0(7)XK and 12.1(2)T.  If you are configuring switched calls or Cisco trunks to Cisco MC3810 multiservice concentrators running Cisco IOS Release 12.0(7)XK and 12.1(2)T and later releases, do not use this option.	
<i>cid</i>	(Optional) Specifies the subchannel to be used for call-control signaling. Valid values are from 4 to 255; the default is 5. If <b>call-control</b> is specified and a CID is not entered, the default CID will be used.	

## voice call send-alert

To enable the terminating gateway to send an alert message instead of a progress message after it receives a call setup message, use the **voice call send-alert** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

**voice call send-alert**

**no voice call send-alert**

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

## voice-card

To configure a voice card, use the **voice-card** command in global configuration mode.

**voice-card** *slot*

---

### Syntax Description

*slot*

On the Cisco 2600 and 3600 platforms, a value from 0 to 3 that identifies the physical slot in the chassis in which the voice card is located.

On Cisco MC3810 mutliservice concentrators with one or two HCMs installed, enter 0 only; this applies to the entire chassis.

---

## voice class busyout

To create a voice class for local voice busyout functions, use the **voice class busyout** command in global configuration mode. To delete the voice class, use the **no** form of this command.

**voice class busyout** *tag*

**no voice class busyout** *tag*

---

### Syntax Description

*tag*

A unique identification number assigned to one voice class. The range is 1 to 10,000.

---

## voice class codec

To enter voice-class configuration mode and assign an identification tag number for a codec voice class, use the **voice class codec** command in global configuration mode. To delete a codec voice class, use the **no** form of this command.

**voice class codec** *tag*

**no voice class codec** *tag*

---

### Syntax Description

*tag*

The unique number you assign to the voice class. The valid range is 1 to 10,000. Each tag number must be unique on the router.

---

## voice-class codec

To assign a previously configured codec selection preference list (codec voice class) to a VoIP dial peer, enter the **voice-class codec** command in dial-peer configuration mode. To remove the codec preference assignment from the dial peer, use the **no** form of this command.

**voice-class codec** *tag*

**no voice-class codec** *tag*

---

<b>Syntax Description</b>	<i>tag</i>	The unique number assigned to the voice class. The valid range for this tag is 1 to 10,000. The <i>tag</i> number maps to the tag number created using the <b>voice class codec</b> global configuration command.
---------------------------	------------	---

---

## voice class dualtone

To create a voice class for Foreign Exchange Office (FXO) supervisory disconnect tone detection parameters, use the **voice class dualtone** command in global configuration mode. To delete the voice class, use the **no** form of this command.

**voice class dualtone** *tag*

**no voice class dualtone** *tag*

---

<b>Syntax Description</b>	<i>tag</i>	A unique identification number assigned to one voice class. The range is from 1 to 10,000.
---------------------------	------------	--

---

## voice class h323

To create an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers, use the **voice class h323** command in global configuration mode. To remove the voice class, use the **no** form of this command.

**voice class h323** *tag*

**no voice class h323**

---

<b>Syntax Description</b>	<i>tag</i>	Specifies a number to identify the voice class. The valid range for this tag is 1 to 10,000. The tag number must be unique on the router.
---------------------------	------------	---

---

## voice-class h323 (dial peer)

To assign an H.323 voice class to a VoIP dial peer, use the **voice-class h323** command in dial-peer configuration mode. To remove the voice class from the dial peer, use the **no** form of this command.

**voice-class h323** *tag*

**no voice-class h323** *tag*

<b>Syntax Description</b>	<i>tag</i>	Specifies a number to identify the voice class. The valid range for this tag is 1 to 10,000. The tag number must be unique on the router.
---------------------------	------------	---

## voice class permanent

To create a voice class for a Cisco trunk or FRF.11 trunk, use the **voice class permanent** command in global configuration mode. To delete the voice class, use the **no** form of this command.

**voice class permanent** *tag*

**no voice class permanent** *tag*

<b>Syntax Description</b>	<i>tag</i>	The unique number that you assign to the voice class. The <i>tag</i> number must be unique on the router. The valid range for this tag is 1 to 10,000.
---------------------------	------------	--

## voice-class permanent (dial-peer)

To assign a previously configured voice class for a Cisco trunk or FRF.11 trunk to a network dial peer, use the **voice-class permanent** command in dial-peer configuration mode. To remove the voice-class assignment from the network dial peer, use the **no** form of this command.

**voice-class permanent** *tag*

**no voice-class permanent** *tag*

<b>Syntax Description</b>	<i>tag</i>	The unique number assigned to the voice class. The <i>tag</i> number maps to the tag number created using the <b>voice class permanent</b> global configuration command. The valid range is from 1 to 10,000.
---------------------------	------------	---

## voice-class permanent

To assign a previously configured voice class for a Cisco trunk or FRF.11 trunk to a voice port, use the **voice-class permanent** command in voice-port configuration mode. To remove the voice-class assignment from the voice port, use the **no** form of this command.

**voice-class permanent** *tag*

**no voice-class permanent** *tag*

---

<b>Syntax Description</b>	<i>tag</i>	The unique number assigned to the voice class. The <i>tag</i> number maps to the tag number created using the <b>voice class permanent</b> global configuration command. The valid range is from 1 to 10,000.
---------------------------	------------	---

---

## voice confirmation-tone

To disable the two-beep confirmation tone for private line, automatic ringdown (PLAR) or PLAR off premises extension (OPX) connections, use the **voice confirmation-tone** command in voice-port configuration mode. To enable the two-beep confirmation tone, use the **no** form of this command.

**voice confirmation-tone**

**no voice confirmation-tone**

---

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

## voice-encap

This command was added in Cisco IOS Release 11.3(1)MA on the Cisco MC3810 multiservice concentrator. This command is not supported in Cisco IOS Release 12.2.

## voice-group

This command was added in Cisco IOS Release 11.3(1)MA for the Cisco MC3810 multiservice concentrator. This command is not supported in Cisco IOS Release 12.2.

## voice hunt user-busy

To configure an originating or tandem router so that it continues dial-peer hunting if it receives a user-busy disconnect code from a destination router, use the **voice hunt user-busy** command in global configuration mode. To configure the router so that it stops dial-peer hunting if it receives a user-busy disconnect code (the default option), use the **no** form of this command.

**voice hunt user-busy**

**no voice hunt user-busy**

---

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

## voice local-bypass

To configure local calls to bypass the digital signal processor (DSP), use the **voice local-bypass** command in global configuration mode. To direct local calls through the DSP, use the **no** form of this command.

**voice local-bypass**

**no voice local-bypass**

---

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

## voice-port

To enter voice-port configuration mode, use the **voice-port** command in global configuration mode.

### Cisco 1750 Router

**voice-port** *slot-number/port*

### Cisco 2600 and Cisco 3600 Series Router

**voice-port** {*slot-number/subunit-number/port*} | {*slot/port:ds0-group-no*}

### Cisco MC3810 Multiservice Concentrator

**voice-port** *slot/port*

### Cisco AS5300 Universal Access Server

**voice-port** *controller number:D*

**Cisco AS5800 Universal Access Server**

```
voice-port {shelf/slot/port:D} | {shelf/slot/parent:port:D}
```

**Cisco 7200 Series Router**

```
voice-port {slot/port:ds0-group-no} | {slot-number/subunit-number/port}
```

**Syntax Description****For the Cisco 1750 Router**

<i>slot-number</i>	Slot number in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot in which it has been installed.
<i>port</i>	Indicates the voice port. Valid entries are 0 or 1.

**For the Cisco 2600 and Cisco 3600 Series Routers**

<i>slot-number</i>	Slot number in the Cisco router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot where it has been installed.
<i>subunit-number</i>	Subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.
<i>port</i>	Voice port number. Valid entries are 0 or 1.
<i>slot</i>	The router location in which the voice port adapter is installed. Valid entries are from 0 to 3.
<i>port</i>	Indicates the voice interface card location. Valid entries are 0 or 3.
<i>ds0-group-no</i>	Indicates the defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.

**For the Cisco MC3810 Multiservice Concentrator**

<i>slot/port</i>	<p>The <i>slot</i> argument specifies the slot number in the Cisco router in which the VIC is installed. The only valid entry is 1.</p> <p>The <i>port</i> variable specifies the voice port number. Valid ranges are as follows:</p> <ul style="list-style-type: none"> <li>• Analog voice ports: from 1 to 6.</li> <li>• Digital voice port:</li> <li>• Digital T1: from 1 to 24.</li> <li>• Digital E1: from 1 to 15, and from 17 to 31.</li> </ul>
------------------	--

**For the Cisco AS5300 Universal Access Server**

<i>controller number</i>	Specifies the T1 or E1 controller.
<b>:D</b>	Indicates the D channel associated with ISDN PRI.

**For the Cisco AS5800 Universal Access Server**

<i>shelf/slot/port</i>	Specifies the T1 or E1 controller on the T1 card. Valid entries for the <i>shelf</i> argument are 0 to 9999. Valid entries for the <i>slot</i> value is 0 to 11. Valid entries for the <i>port</i> variable is 0 to 11.
<i>shelf/slot/parent:port</i>	Specifies the T1 controller on the T3 card. Valid entries for the <i>shelf</i> argument are 0 to 9999. Valid entries for the <i>slot</i> argument are 0 to 11. Valid entries for the <i>port</i> argument are 1 to 28. The value for the <i>parent</i> argument is always 0.
<b>:D</b>	Indicates the D channel associated with ISDN PRI.

**For the Cisco 7200 Series Router**

<i>slot</i>	The router location in which the voice port adapter is installed. Valid entries are from 0 to 3.
<i>port</i>	Indicates the VIC location. Valid entries are 0 or 1.
<i>dso-group-no</i>	Indicates the defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
<i>slot-number</i>	Indicates the slot number in the Cisco router in which the VIC is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
<i>subunit-number</i>	Indicates the subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.
<i>port</i>	Indicates the voice port number. Valid entries are 0 or 1.

## voice-port busyout

To place all voice ports associated with a serial or ATM interface into a busyout state, use the **voice-port busyout** command in interface configuration mode. To remove the busyout state on the voice ports associated with this interface, use the **no** form of this command.

**voice-port busyout**

**no voice-port busyout**

### Syntax Description

This command has no arguments or keywords.

## voice rtp send-recv

To establish a two-way voice path when the Real-Time Transport Protocol (RTP) channel is opened, use the **voice rtp send-recv** command in global configuration mode. To restore the default condition, use the **no** form of this command.

```
voice rtp send-recv
```

```
no voice rtp send-recv
```

---

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

## voice service

To specify the voice encapsulation type, use the **voice service** command in global configuration mode. To exit voice-service configuration mode, use the **exit** command.

```
voice service { voip | voatm }
```

---

<b>Syntax Description</b>	<b>voip</b>	Specifies Voice over IP (VoIP) parameters.
	<b>voatm</b>	Specifies Voice over ATM (VoATM) parameters.

---

## voice vad-time

To change the minimum silence detection time for voice activity detection (VAD), use the **voice vad-time** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
voice vad-time milliseconds
```

```
no voice vad-time
```

---

<b>Syntax Description</b>	<i>milliseconds</i>	The waiting period, in milliseconds, before silence detection and suppression of voice-packet transmission. The range is 250 to 65,536. The default is 250.
---------------------------	---------------------	---

---

## voip-incoming translation-rule

To set the incoming translation rule for calls that originate from H.323-compatible clients, use the **voip-incoming translation-rule** command in global configuration mode. To disable the incoming translation rule, use the **no** form of this command.

```
voip-incoming translation-rule name-tag { calling-number | called-number }
```

```
no voip-incoming translation-rule name-tag { calling-number | called-number }
```

<b>Syntax Description</b>	<i>name-tag</i>	The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. The range is 1 through 2,147,483,647.
	<b>calling-number</b>	The ANI number or the number of the calling party.
	<b>called-number</b>	The Dial Number Information Service (DNIS) number or the number of the called party.

## zone access

To configure the accessibility of your local-zone zone, use the **zone access** command in gatekeeper configuration mode. To remove any accessibility configurations, use the **no** form of this command.

```
zone access local-zone-name { default | remote-zone remote-zone-name } { direct | proxied }
```

```
no zone access local-zone-name remote-zone remote-zone-name
```

<b>Syntax Description</b>	<i>local-zone-name</i>	Name of local zone (synonymous with local gatekeeper).
	<b>default</b>	Use with the <b>direct</b> or <b>proxied</b> keyword to define the mode of behavior for all remote zones that have not been specially named using the <b>remote-zone</b> <i>remote-zone-name</i> keyword and argument combination.
	<b>remote-zone</b> <i>remote-zone-name</i>	Name of remote zone (synonymous with remote gatekeeper) for which a special mode of behavior is defined.
	<b>direct</b>	Configures direct calls (without use of proxies) between endpoints. The local zone (or gatekeeper) offers the local endpoint IP address instead of the IP address of a local proxy.
	<b>proxied</b>	Configures calls using proxies between endpoints. The local zone (or gatekeeper) offers the IP address of a local proxy instead of the local endpoint address.

## zone bw

To set the maximum bandwidth allowed in a gatekeeper zone at any one time, use the **zone bw** command in gatekeeper configuration mode. To remove the maximum bandwidth setting and make the bandwidth unlimited, use the **no** form of this command.

```
zone bw gatekeeper-name max-bandwidth
```

```
no zone bw gatekeeper-name max-bandwidth
```

<b>Syntax Description</b>	<i>gatekeeper-name</i>	Name of the gatekeeper that controls the zone.
	<i>max-bandwidth</i>	Maximum bidirectional bandwidth, in kbps, allowed in the zone at any one time.

## zone local

To specify a zone controlled by a gatekeeper, use the **zone local** command in gatekeeper configuration mode. To remove a zone controlled by a gatekeeper, use the **no** form of this command.

```
zone local gatekeeper-name domain-name [ras-IP-address]
```

```
no zone local gatekeeper-name domain-name
```

### Syntax Description

<i>gatekeeper-name</i>	The gatekeeper's name or zone name. This is usually the fully domain-qualified host name of the gatekeeper. For example, if the <i>domain-name</i> is cisco.com, the <i>gatekeeper-name</i> might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the <i>gatekeeper-name</i> for each zone should be some unique string that has a mnemonic value.
<i>domain-name</i>	The domain name served by this gatekeeper.
<i>ras-IP-address</i>	(Optional) The IP address of one of the interfaces on the gatekeeper. When the gatekeeper responds to gatekeeper discovery messages, it signals the endpoint or gateway to use this address in future communications.



#### Note

Setting this address for one local zone makes it the address used for all local zones.

## zone prefix

To add a prefix to the gatekeeper zone list, use the **zone prefix** command in gatekeeper configuration mode. To remove knowledge of a zone prefix, use the **no** form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the **no** form of this command with the **gw-priority** option.

```
zone prefix gatekeeper-name e164-prefix [blast | seq] [gw-priority priority gw-alias  
[gw-alias, ...]]
```

```
no zone prefix gatekeeper-name e164-prefix [blast | seq] [gw-priority priority gw-alias  
[gw-alias, ...]]
```

**Syntax Description**

*gatekeeper-name* The name of a local or remote gatekeeper, which must have been defined by using the **zone local** or **zone remote** command.

*e164-prefix* An E.164 prefix in standard form followed by dots (.). Each dot represents a number in the E.164 address. For example, 212..... is matched by 212 and any seven numbers.



**Note** Although a dot representing each digit in an E.164 address is the preferred configuration method, you can also enter an asterisk (\*) to match any number of digits.

**blast** (Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent simultaneously to the gatekeepers based on the order in which they were listed. The default is **seq**.

**seq** (Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which they were listed. The default is **seq**.

**gw-priority** (Optional) Use the **gw-priority** option to define how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix *e164-prefix*. Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper.

*pri-0-to-10 gw-alias*

Use values from 0 to 10. A 0 value prevents the gatekeeper from using the gateway *gw-alias* for that prefix. Value 10 places the highest priority on gateway *gw-alias*. If you do not specify a priority value for a gateway, the value 5 is assigned.

To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the *pri-0-to-10* value.

The *gw-alias* name is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This name is set on the gateway with the **h323-gateway voip h.323-id** command.

## zone remote

To statically specify a remote zone if domain name service (DNS) is unavailable or undesirable, use the **zone remote** command in gatekeeper configuration mode. To remove the remote zone, use the **no** form of this command.

**zone remote** *other-gatekeeper-name other-domain-name other-gatekeeper-ip-address*  
[*port-number*]

**no zone remote** *other-gatekeeper-name other-domain-name other-gatekeeper-ip-address*  
[*port-number*]

**Syntax Description**

*other-gatekeeper-name* Name of the remote gatekeeper.

*other-domain-name* Domain name of the remote gatekeeper.

<i>other-gatekeeper-ip-address</i>	IP address of the remote gatekeeper.
<i>port-number</i>	(Optional) RAS signaling port number for the remote zone. Value ranges from 1 to 65,535. If this is not set, the default is the well-known RAS port number 1719.

## zone subnet

To configure a gatekeeper to accept discovery and registration messages sent by endpoints in designated subnets, use the **zone subnet** command in gatekeeper configuration mode. To disable the gatekeeper from acknowledging discovery and registration messages from subnets or to remove subnets entirely, use the **no** form of this command.

```
zone subnet local-gatekeeper-name { default | subnet-address {/bits-in-mask | mask-address} }
enable
```

```
no zone subnet local-gatekeeper-name { default | subnet-address {/bits-in-mask | mask-address} }
enable
```

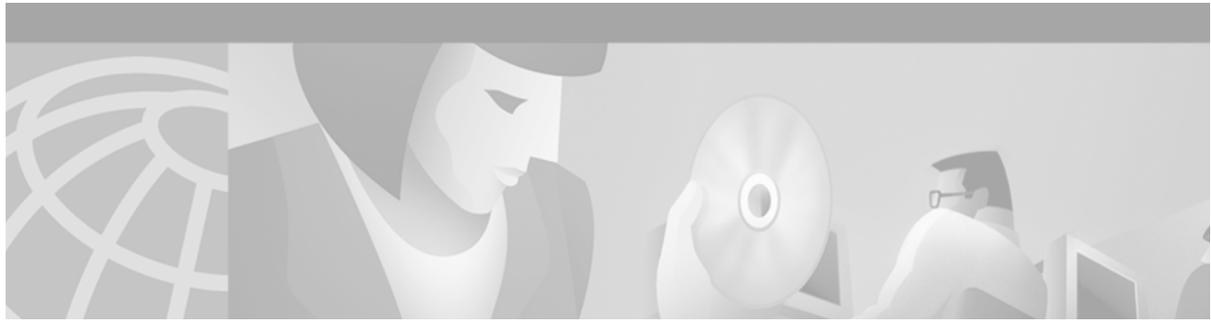
Syntax Description	
<i>local-gatekeeper-name</i>	Name of the local gatekeeper.
<b>default</b>	Applies to all other subnets that are not specifically defined by the <b>zone subnet</b> command.
<i>subnet-address</i>	Address of the subnet being defined.
<i>/bits-in-mask</i>	Number of bits of the mask to be applied to the subnet address.
<i>mask-address</i>	Mask (in dotted string format) to be applied to the subnet address.
<b>enable</b>	Gatekeeper accepts discovery and registration from the specified subnets.





**Mobile Wireless**





## Mobile Wireless Commands

---

This chapter describes the function and syntax of the mobile wireless commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Mobile Wireless Command Reference*.

### access-mode

To specify whether the GGSN requests user authentication at the access point to a PDN, use the **access-mode** access-point configuration command. To remove an access mode, use the **no** form of the command.

**access-mode** { **transparent** | **non-transparent** }

**no access-mode** { **transparent** | **non-transparent** }

Syntax Description		
	<b>transparent</b>	Specifies that the users who access the PDN through the access point associated with the current virtual template are allowed access without authorization or authentication.
	<b>non-transparent</b>	Specifies that users who access the PDN through the current virtual template must be authenticated by the GGSN acting as a proxy for the authentication.

### access-point

To specify an access point number and enter access-point configuration mode, use the **access-point** access-point list configuration command. To delete an access point number, use the **no** form of the command.

**access-point** *ap\_number*

**no access-point** *ap\_number*

Syntax Description		
	<i>ap_number</i>	Integer from 0 to 4,294,967,295 ( $2^{32}-1$ ) that identifies a GPRS access point.

## access-point-name

To specify the network (or domain) name for a PDN that users can access from the GGSN at a defined access point, use the **access-point-name** access-point configuration command. To delete a current access point name, use the **no** form of the command.

**access-point-name** *apn\_name*

**no access-point-name** *apn\_name*

---

### Syntax Description

<i>apn_name</i>	Specifies the network or domain name for a private data network that can be accessed through the current access point.
-----------------	--

---

## access-violation

To specify the action to take when a user attempts unauthorized access to a PDN through an access point, use the **access-violation** access-point configuration command. To restore the default value for the command, use the **no** form of the command.

**access-violation** { **discard-packets** | **deactivate-pdp-context** }

**no access-violation** { **discard-packets** | **deactivate-pdp-context** }

---

### Syntax Description

<b>discard-packets</b>	Specifies that user packets are discarded when an unauthorized access attempt is detected.
<b>deactivate-pdp-context</b>	Specifies that the user's session is ended when an unauthorized access attempt is detected.

---

## clear gprs charging cdr

To clear GPRS call detail records (CDRs), use the **clear gprs charging cdr** privileged EXEC configuration command.

**clear gprs charging cdr** { **tid** *tunnel-id* | **access-point** *access-point-index* | **all** }

---

### Syntax Description

<b>tid</b> <i>tunnel-id</i>	Tunnel ID of the connection for which to clear charging CDRs.
<b>access-point</b> <i>access-point-index</i>	Specifies clearing the CDRs for a specified access-point index.
<b>all</b>	Specifies clearing all CDRs on the GGSN.

---

## clear gprs gtp pdp-context

To clear one or more PDP contexts (mobile sessions), use the **clear gprs gtp pdp-context** privileged EXEC configuration command.

```
clear gprs gtp pdp-context {tid tunnel-id | imsi imsi_value | path ip-address | access-point
access-point-index | all}
```

Syntax Description		
	<b>tid</b> <i>tunnel-id</i>	Tunnel ID (TID) for which PDP contexts are to be cleared.
	<b>imsi</b> <i>imsi_value</i>	International Mobile Subscriber Identity (IMSI) value for which PDP contexts are to be cleared.
	<b>path</b> <i>ip-address</i>	Remote GSN IP address for which all PDP contexts associated with the GSN are to be cleared.
	<b>access-point</b> <i>access-point-index</i>	Access-point index for which PDP contexts are to be cleared.
	<b>all</b>	Clear all currently active PDP contexts.

## clear gprs gtp statistics

To clear the current GPRS GTP statistics, use the **clear gprs gtp statistics** privileged EXEC configuration command.

```
clear gprs gtp statistics
```

Syntax Description	
	This command has no arguments or keywords.

## dhcp-gateway-address

To specify the address returned by the DHCP server in DHCP requests for MS users entering a particular PDN access point, use the **dhcp-gateway-address** access-point configuration command. To restore the default setting for the command (to use the virtual template interface address), use the **no** form of the command.

```
dhcp-gateway-address ip-address
```

```
no dhcp-gateway-address ip-address
```

Syntax Description		
	<i>ip-address</i>	The IP address of the DHCP gateway to be used in DHCP requests for users who connect through the specified access point.

## dhcp-server

To specify a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point, use the **dhcp-server** access-point configuration command. To delete the DHCP server from the access-point configuration, use the **no** form of the command.

```
dhcp-server { ip-address | name } [ip-address | name]
```

```
no dhcp-server { ip-address | name } [ip-address | name]
```

<b>Syntax Description</b>	<i>ip-address</i>	IP address of a DHCP server. The first <i>ip-address</i> argument specifies the IP address of the primary DHCP server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup DHCP server.
	<i>name</i>	Host name of a DHCP server. The second (optional) <i>name</i> argument specifies the host name of a backup DHCP server.

## encapsulation gtp

To specify the GPRS tunneling protocol (GTP) as the encapsulation type for packets transmitted over the virtual template interface, use the **encapsulation gtp** interface configuration command. To delete this encapsulation type, use the **no** form of the command.

```
encapsulation gtp
```

```
no encapsulation gtp
```

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

## gprs access-point-list

To configure an access point list that you use to define PDN access points on the GGSN, use the **gprs access-point-list** global configuration command. To delete an existing access-point list, use the **no** form of the command.

```
gprs access-point-list list_name
```

```
no gprs access-point-list list_name
```

<b>Syntax Description</b>	<i>list_name</i>	The name of the access-point list.
---------------------------	------------------	------------------------------------

## gprs canonical-qos best-effort bandwidth-factor

To specify the bandwidth factor to be applied to the canonical best-effort Quality of Service (QoS) class, use the **gprs canonical-qos best-effort bandwidth-factor** global configuration command. To restore the default value for this command, use the **no** form of the command.

```
gprs canonical-qos best-effort bandwidth-factor bandwidth_factor
```

```
no gprs canonical-qos best-effort bandwidth-factor bandwidth_factor
```

---

### Syntax Description

<i>bandwidth_factor</i>	Integer from 1 to 4000000 that specifies the desired bandwidth factor (in bits per second). The default is 10 bits per second.
-------------------------	--

---

## gprs canonical-qos gsn-resource-factor

To specify a value that is used by the GGSN to calculate the QoS level provided to mobile users, use the **gprs canonical-qos gsn-resource-factor** global configuration command. To restore the default value of the command, use the **no** form of the command.

```
gprs canonical-qos gsn-resource-factor resource-factor
```

```
no gprs canonical-qos gsn-resource-factor resource-factor
```

---

### Syntax Description

<i>resource-factor</i>	Integer between 1 and 4294967295 representing the bits per second that the GGSN can handle. The default value is 1048576.
------------------------	---

---

## gprs canonical-qos map tos

To specify a QoS mapping from the canonical QoS classes to an IP type of service (ToS) category, use the **gprs canonical-qos map tos** global configuration command. To remove a QoS mapping, use the **no** form of the command.

```
gprs canonical-qos map tos [premium tos_value [normal tos_value [best-effort tos_value]]]
```

```
no gprs canonical-qos map tos [premium tos_value [normal tos_value [best-effort tos_value]]]
```

---

### Syntax Description

<b>premium</b> <i>tos_value</i>	ToS mapping for a premium QoS. The <i>tos_value</i> can be a number from 0 to 5. A higher number indicates a higher service priority.
<b>normal</b> <i>tos_value</i>	ToS mapping for a normal QoS. The <i>tos_value</i> can be a number from 0 to 5. A higher number indicates a higher service priority.
<b>best-effort</b> <i>tos_value</i>	ToS mapping for a best effort QoS. The <i>tos_value</i> can be a number from 0 to 5. A higher number indicates a higher service priority.

---

## gprs canonical-qos premium mean-throughput-deviation

To specify a mean throughput deviation factor that the GGSN uses to calculate the allowable data throughput for QoS, use the **gprs canonical-qos premium mean-throughput-deviation** global configuration command. To restore the default value for the command (100), use the **no** form of the command.

**gprs canonical-qos premium mean-throughput-deviation** *deviation\_factor*

**no gprs canonical-qos premium mean-throughput-deviation** *deviation\_factor*

<b>Syntax Description</b>	<i>deviation_factor</i>	Value that specifies the deviation factor. This value can range from 1 to 1000. The default value is 100.
---------------------------	-------------------------	---

## gprs charging cdr-aggregation-limit

To specify the maximum number of call detail records (CDRs) that the GGSN aggregates in a charging data transfer message to a charging gateway, use the **gprs charging cdr-aggregation-limit** global configuration command. To restore the default value for this command (255 CDRs), use the **no** form of the command.

**gprs charging cdr-aggregation-limit** *CDR\_limit*

**no gprs charging cdr-aggregation-limit** *CDR\_limit*

<b>Syntax Description</b>	<i>CDR_limit</i>	An integer between 1 and 255 that specifies the number of CDRs that can be accumulated in a charging data transfer message. The default is 255 CDRs.
---------------------------	------------------	--

## gprs charging cdr-option local-record-sequence-number

To specify that the local record sequence number field is used in CDRs on the GGSN, use the **gprs charging cdr-option local-record-sequence-number** global configuration command. To disable this feature, use the **no** form of the command.

**gprs charging cdr-option local-record-sequence-number**

**no gprs charging cdr-option local-record-sequence-number**

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

## gprs charging cdr-option node-id

To specify that the GGSN uses the node ID field in CDRs, use the **gprs charging cdr-option node-id** global configuration command. To disable this feature use the **no** form of the command.

**gprs charging cdr-option node-id**

**no gprs charging cdr-option node-id**

---

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

## gprs charging cg-path-requests

To specify the number of minutes that the GGSN waits before trying to establish the TCP path to the charging gateway when TCP is the specified path protocol, use the **gprs charging cg-path-requests** global configuration command. To restore the default value of 0 minutes and disable the timer, use the **no** form of the command.

**gprs charging cg-path-requests** *minutes*

**no gprs charging cg-path-requests**

---

<b>Syntax Description</b>	<i>minutes</i>	Number of minutes the GGSN waits before retrying a charging request. The default value is 0 minutes, which disables the timer.
---------------------------	----------------	--

---

## gprs charging container volume-threshold

To specify the maximum number of bytes that the GGSN maintains in a user's charging container before closing it and updating the CDR, use the **gprs charging container volume-threshold** global configuration command. To restore the default value for the command (1 megabyte), use the **no** form of the command.

**gprs charging container volume-threshold** *threshold\_value*

**no gprs charging container volume-threshold** *threshold\_value*

---

<b>Syntax Description</b>	<i>threshold_value</i>	A value between 1 and 4294967295 that specifies the container threshold value, in bytes. The default is 1,048,576 bytes (1 MB).
---------------------------	------------------------	---

---

## gprs charging disable

To disable charging transactions on the GGSN, use the **gprs charging disable** global configuration command. To enable charging transactions, use the **no** form of the command.

**gprs charging disable**

**no gprs charging disable**

---

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

## gprs charging flow-control private-echo

To implement an echo request with private extensions for maintaining flow control on packets transmitted to the charging gateway, use the **gprs charging flow-control private-echo** global configuration command. To disable private extensions for flow control, use the **no** form of the command.

**gprs charging flow-control private-echo**

**no gprs charging flow-control private-echo**

---

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

## gprs charging map data tos

To specify an IP ToS mapping for GPRS charging packets, use the **gprs charging map data tos** global configuration command. To restore the default value for the command (3) use the **no** form of the command.

**gprs charging map data tos** *tos\_value*

**no gprs charging map data tos** *tos\_value*

---

<b>Syntax Description</b>	<i>tos_value</i>	Specifies a ToS mapping value between 0 and 5. A higher number indicates a higher service priority. The default value is 3.
---------------------------	------------------	---

---

## gprs charging packet-queue-size

To specify the maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue, use the **gprs charging packet-queue-size** global configuration command. To restore the default value for this command, use the **no** form of the command.

**gprs charging packet-queue-size** *queue\_size*

**no gprs charging packet-queue-size** *queue\_size*

### Syntax Description

<i>queue_size</i>	Value between 1 and 512 that specifies the maximum queue size for the GGSN charging packet data queue. The default is 128 packets.
-------------------	--

## gprs charging path-protocol

To specify the protocol that the GGSN uses to transmit and receive charging data, use the **gprs charging path-protocol** global configuration command. To restore the default value for the command (UDP), use the **no** form of the command.

**gprs charging path-protocol** {**udp** | **tcp**}

**no gprs charging path-protocol** {**udp** | **tcp**}

### Syntax Description

<b>udp</b>	User Datagram Protocol, which is a connectionless transport protocol.
<b>tcp</b>	Transport Control Protocol, which is a connection-based transport protocol.

## gprs charging server-switch-timer

To specify a timeout value that determines when the GGSN attempts to find an alternate charging gateway after a destination charging gateway cannot be located or becomes unusable, use the **gprs charging server-switch-timer** global configuration command. To restore the default value for this command (60 seconds), use the **no** form of the command.

**gprs charging server-switch-timer** *seconds*

**no gprs charging server-switch-timer** *seconds*

### Syntax Description

<i>seconds</i>	Timeout value (between 0 and 300 seconds), that the GGSN waits before attempting to contact an alternate charging gateway. The default value is 60 seconds.
----------------	---

## gprs charging tariff-time

To specify a time of day when GPRS charging tariffs change, use the **gprs charging tariff-time** global configuration command. To delete an existing tariff time, use the **no** form of the command. You can set up a maximum of 32 tariff change times.

**gprs charging tariff-time** *time*

**no gprs charging tariff-time** *time*

<b>Syntax Description</b>	<i>time</i>	A time of day when the charging tariff changes. Specify the time format as hh:mm:ss.
---------------------------	-------------	--

## gprs charging transfer interval

To specify the number of seconds that the GGSN waits before it transfers charging data to the charging gateway, use the **gprs charging transfer interval** global configuration command. To restore the default setting for the transfer interval, use the **no** form of the command.

**gprs charging transfer interval** *seconds*

**no gprs charging transfer interval**

<b>Syntax Description</b>	<i>seconds</i>	Interval between charging transfers, in seconds. Can be a value between 1 and 4294967295 seconds. The default is 105 seconds.
---------------------------	----------------	---

## gprs default charging-gateway

To specify the default charging gateway, use the **gprs default charging gateway** global configuration command. To delete the charging gateways, use the **no** form of the command.

**gprs default charging-gateway** {*ip-address* | *name*} [{*ip-address* | *name*}]

**no gprs default charging-gateway** {*ip-address* | *name*} [{*ip-address* | *name*}]

<b>Syntax Description</b>	<i>ip-address</i>	IP address of a default gateway.
	<i>name</i>	Host name for a default gateway.

## gprs default dhcp-server

To specify a default Dynamic Host Configuration Protocol (DHCP) server from which the GGSN obtains IP address leases for mobile users, use the **gprs default dhcp-server** global configuration command. To delete the default DHCP server, use the **no** form of the command.

```
gprs default dhcp-server {ip-address | name} [{ip-address | name}]
```

```
no gprs default dhcp-server {ip-address | name} [{ip-address | name}]
```

Syntax Description		
<i>ip-address</i>		IP address of a DHCP server. The first IP address is the name of the primary DHCP server. The second (optional) <i>ip_address</i> argument specifies the IP address of a backup DHCP server.
<i>name</i>		Host name of a DHCP server. The second (optional) <i>name</i> argument specifies the host name of a backup DHCP server.

## gprs default ip-address-pool

To specify a dynamic address allocation method using IP address pools for the GGSN, use the **gprs default ip-address-pool** global configuration command. To disable the address allocation method, use the **no** form of the command.

```
gprs default ip-address-pool {dhcp-proxy-client | disable | radius-client}
```

```
no gprs default ip-address-pool {dhcp-proxy-client | disable | radius-client}
```

Syntax Description		
<b>dhcp-proxy-client</b>		GGSN dynamically acquires IP addresses for an MS from a DHCP server.
<b>disable</b>		Disables dynamic address allocation by the GGSN.
<b>radius-client</b>		GGSN dynamically acquires IP addresses for an MS from a RADIUS server.

## gprs default radius-server

To specify a primary (and backup) RADIUS server that the GGSN uses to authenticate mobile users for access to PDNs, use the **gprs default radius-server** global configuration command. To delete the RADIUS server identification, use the **no** form of the command.

```
gprs default radius-server {ip-address | name} [{ip-address | name}]
```

```
no gprs default radius-server {ip-address | name} [{ip-address | name}]
```

Syntax Description		
<i>ip-address</i>		IP address of a RADIUS server. The first IP address is the name of the primary RADIUS server. The second (optional) <i>ip_address</i> argument specifies the IP address of a backup RADIUS server.
<i>name</i>		Host name of a RADIUS server. The second (optional) <i>name</i> argument specifies the host name of a backup RADIUS server.

## gprs fastswitch

To enable the GPRS fast switching feature on the GGSN, use the **gprs fastswitch** command. To disable fast switching, use the **no** form of the command.

**gprs fastswitch**

**no gprs fastswitch**

---

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

## gprs gtp error-indication throttle

To specify the maximum number of error indication messages that the GGSN sends out in one second, use the **gprs gtp error-indication throttle** command. To restore the default value (no error indication throttle is used), use the **no** form of the command (GGSN only).

**gprs gtp error-indication throttle window-size** *size*

**no gprs gtp error-indication throttle**

---

**Syntax Description** **window-size** *size* Counter that is decremented when an error indication message is sent and reset to the configured value after one second, with a value between 0 and 256.

---

## gprs gtp map signalling tos

To specify an IP ToS mapping for GPRS tunneling protocol (GTP) signaling packets, use the **gprs gtp map signalling tos** global configuration command. To restore the default value for the command (5) use the **no** form of the command.

**gprs gtp map signalling tos** *tos\_value*

**no gprs gtp map signalling tos** *tos\_value*

---

**Syntax Description** *tos\_value* Value between 0 and 7 that specifies the IP ToS mapping. The default value is 5.

---

## gprs gtp n3-buffer-size

To specify the size of the receive buffer that the GGSN uses to receive GTP signaling messages and packets sent through the tunneling protocol, use the **gprs gtp n3-buffer-size** global configuration command. To restore the default value for the N3 buffer, use the **no** form of the command.

**gprs gtp n3-buffer-size** *bytes*

**no gprs gtp n3-buffer-size**

<b>Syntax Description</b>	<i>bytes</i>	Value between 2048 and 65535 that specifies the size of the N3 buffer, in bytes. The default is 8192 bytes.
---------------------------	--------------	---

## gprs gtp n3-requests

To specify the maximum number of times that the GGSN attempts to send a signaling request, use the **gprs gtp n3-requests** global configuration command. To restore the default value (5 request attempts), use the **no** form of the command.

**gprs gtp n3-requests** *requests*

**no gprs gtp n3-requests** *requests*

<b>Syntax Description</b>	<i>requests</i>	A number between 1 and 65535 that specifies the number of times a request is attempted. The default is 5 requests.
---------------------------	-----------------	--

## gprs gtp path-echo-interval

To specify the number of seconds that the GGSN waits before sending an echo-request message to check for GTP path failure, use the **gprs gtp path-echo-interval** global configuration command. To restore the default value for the path echo interval (60 seconds), use the **no** form of the command.

**gprs gtp path-echo-interval** *interval*

**no gprs gtp path-echo-interval** *interval*

<b>Syntax Description</b>	<i>interval</i>	Number of seconds that the GGSN waits before sending an echo-request message. Specify a value between 60 and 65535 seconds. The value 0 disables the echo-request feature. The default is 60 seconds.
---------------------------	-----------------	---

## gprs gtp t3-response

To specify the maximum time that the GGSN waits to respond to a signaling request message, use the **gprs gtp t3-response** global configuration command. To restore the default value for the response interval (1 second), use the **no** form of the command.

```
gprs gtp t3-response response_interval
```

```
no gprs gtp t3-response response_interval
```

---

### Syntax Description

*response\_interval* A value between 1 and 65535 that specifies the length of the T3 response interval, in seconds. The default is 1 second.

---

## gprs gtp t3-tunnel

To specify the length of time that the GGSN waits, after receiving a GTP context request message from the SGSN and before forwarding a protocol data unit (PDU) to the requesting SGSN, use the **gprs gtp t3-tunnel** global configuration command. To restore the default value for the command (20 seconds), use the **no** form of the command.

```
gprs gtp t3-tunnel seconds
```

```
no gprs gtp t3-tunnel seconds
```

---

### Syntax Description

*seconds* A value between 1 and 65535 that specifies the interval the GGSN waits before forwarding a PDU to a requesting SGSN. The default is 20 seconds.

---

## gprs idle-pdp-context purge-timer

To specify the time that the GGSN waits before purging idle mobile sessions, use the **gprs idle-pdp-context purge-timer** global configuration command. To restore the default value for the command (72 hours), use the **no** form of the command.

```
gprs idle-pdp-context purge-timer hours
```

```
no gprs idle-pdp-context purge-timer hours
```

---

### Syntax Description

*hours* Value between 0 and 255 that specifies the number of hours that the GGSN waits before purging idle sessions. The value 0 disables the purge timer. The default is 72 hours.

---

## gprs maximum-pdp-context-allowed

To specify the maximum number of PDP contexts (mobile sessions) that can be activated on the GGSN, use the **gprs maximum-pdp-context-allowed** global configuration command. To restore the default value for the command (1000 PDP contexts), use the **no** form of the command.

```
gprs maximum-pdp-context-allowed pdp_contexts
```

```
no gprs maximum-pdp-context-allowed pdp_contexts
```

---

**Syntax Description**

*pdp\_contexts*

Integer between 1 and 4296967295 that specifies the number of active PDP contexts allowed. The default is 1000 PDP contexts.

---

## gprs qos default-response requested

To configure the GGSN to set its default QoS values in the response message exactly as requested in the create PDP context request message, use the **gprs qos default-response requested** global configuration command. To return the GGSN to its QoS default of best-effort, use the **no** form of this command.

```
gprs qos default-response requested
```

```
no gprs qos default-response requested
```

---

**Syntax Description**

This command has no arguments or keywords.

## gprs qos map canonical-qos

To enable mapping of GPRS QoS categories to a canonical QoS method that includes best-effort, normal, and premium QoS classes, use the **gprs qos map canonical-qos** global configuration command. To disable this mapping, use the **no** form of the command.

```
gprs qos map canonical-qos
```

```
no gprs qos map canonical-qos
```

---

**Syntax Description**

This command has no arguments or keywords.

## gprs radius msisdn first-byte

To specify that the first byte of the Mobile Stations International PSTN/ISDN (MSISDN) information element (IE) is included in a Remote Access Dial-In User Service (RADIUS) request, use the **gprs radius msisdn first-byte** global configuration command. To remove the first byte from the MSISDN IE in a RADIUS request, use the **no** form of the command.

**gprs radius msisdn first-byte**

**no gprs radius msisdn first-byte**

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

## ip-access-group

To specify access permissions between an MS and a PDN through the GGSN at a particular access point, use the **ip-access-group** access-point configuration command. To disable the input access list, use the **no** form of the command.

**ip-access-group** *access\_list\_number* { **in** | **out** }

**no ip-access-group** *access\_list\_number* { **in** | **out** }

<b>Syntax Description</b>	<i>access_list_number</i> Number of an access list that has been set up using the <b>access-list</b> command.
<b>in</b>	The specified access list controls access from the PDN to the mobile station.
<b>out</b>	The specified access list controls access from the mobile station to the PDN.

## ip-address-pool

To specify a dynamic address allocation method using IP address pools for the current access point, use the **ip-address-pool** access-point configuration command. To restore the default value (to use the globally defined address-allocation method, which is set using the **gprs default ip-address-pool** command), use the **no** form of the command.

**ip-address-pool** { **dhcp-proxy-client** | **radius-client** | **disable** }

**no ip-address-pool** { **dhcp-proxy-client** | **radius-client** | **disable** }

<b>Syntax Description</b>	<b>dhcp-proxy-client</b> The access-point IP address pool is allocated using a DHCP server.
	<b>radius-client</b> The access-point IP address pool is allocated using a RADIUS server.
	<b>disable</b> Disables dynamic address allocation for this access point.

## protocol-type

To specify the protocol type for the current access point, use the **protocol-type** access-point configuration command.

**protocol-type ip**

**no protocol-type ip**

Syntax Description	ip	Specifies that the access point will use the IP protocol
--------------------	----	--

## radius-server

To specify a primary (and backup) RADIUS server that the GGSN uses at a particular access point to authenticate mobile users for access to a PDN, use the **radius-server** access-point configuration command. To delete the RADIUS server identification, use the **no** form of the command.

**radius-server** {*ip-address* | *name*} [{*ip-address* | *name*}]

**no radius-server** {*ip-address* | *name*} [{*ip-address* | *name*}]

Syntax Description	<i>ip-address</i>	IP address of a RADIUS server. The first IP address is the name of the primary RADIUS server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup RADIUS server.
	<i>name</i>	Host name of a RADIUS server. The second (optional) <i>name</i> argument specifies the host name of a backup RADIUS server.

## service gprs

To specify the type of GPRS support node that is enabled on the router, use the **service gprs** command. To disable GPRS support node functionality, use the **no** form of the command.

**service gprs** {*sgsn-datacom* | *ggsn*}

**no service gprs** {*sgsn-datacom* | *ggsn*}

Syntax Description	<i>sgsn-datacom</i>	Specifies that the router will function as a Serving GPRS Support Node (SGSN) datacom unit.
	<i>ggsn</i>	Specifies that the router will function as a Gateway GPRS Support Node (GGSN).

## show gprs access-point

To obtain information about access points on the GGSN, use the **show gprs access-point** privileged EXEC command.

```
show gprs access-point [access-point-index] [address-allocation] [all]
```

<b>Syntax Description</b>	<i>access-point-index</i>	Index number of an access point. Information about that access point is shown.
	<b>address-allocation</b>	Information about dynamically allocated mobile station (MS) addresses and lease terms for the access point is shown.
	<b>all</b>	Information about all access points on the GGSN is shown.

## show gprs charging parameters

To display information about the current GPRS charging configuration, use the **show gprs charging parameters** privileged EXEC command.

```
show gprs charging parameters
```

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

## show gprs charging statistics

To display current statistics about the transfer of charging packets between the GGSN and charging gateways, use the **show gprs charging statistics** privileged EXEC command.

```
show gprs charging statistics { tid tunnel_id | access-point access-point-index | all }
```

<b>Syntax Description</b>	<b>tid</b> <i>tunnel_id</i>	Specifies a tunnel ID for which you want to display charging statistics.
	<b>access-point</b> <i>access-point-index</i>	Specifies the index of the access point for which you want to display statistics.
	<b>all</b>	Requests display of all charging statistics.

## show gprs gtp parameters

To display information about the current GPRS Tunneling Protocol (GTP) configuration on the GGSN, use the **show gprs gtp parameters** privileged EXEC command.

```
show gprs gtp parameters
```

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

## show gprs gtp path

To display information about one or more GTP paths between the GGSN and other GPRS devices, use the **show gprs gtp path** privileged EXEC command.

```
show gprs gtp path {ip-address | all}
```

### Syntax Description

<i>ip-address</i>	Displays GTP path information for a specified IP address.
<b>all</b>	Displays information for all GTP paths.

## show gprs gtp pdp-context

To display a list of the currently active PDP contexts (mobile sessions), use the **show gprs gtp pdp-context** privileged EXEC command.

```
show gprs gtp pdp-context {tid tunnel_id | imsi imsi | path ip-address | access-point  
access-point-index | pdp-type ip | qos-precedence {low | normal | high} | all}
```

### Syntax Description

<b>tid</b> <i>tunnel_id</i>	Displays PDP contexts by tunnel ID.
<b>imsi</b> <i>imsi</i>	Displays PDP contexts by International Mobile Subscriber Identity (IMSI).
<b>path</b> <i>ip-address</i>	Displays PDP contexts by IP address.
<b>access-point</b> <i>access-point-index</i>	Displays PDP contexts by access point.
<b>pdp-type</b> <b>ip</b>	Displays PDP contexts that are transmitted via IP.
<b>qos-precedence</b>	Displays PDP contexts for a specified GPRS quality of service precedence type. You can specify the following precedence types: <b>low</b> , <b>normal</b> , or <b>high</b> .
<b>all</b>	Displays all PDP contexts.

## show gprs gtp statistics

To display the current GPRS Tunneling Protocol (GTP) statistics for the GGSN (such as IE, GTP signaling, and GTP PDU statistics), use the **show gprs gtp statistics** privileged EXEC command.

```
show gprs gtp statistics
```

### Syntax Description

This command has no arguments or keywords.

## show gprs gtp status

To display information about the current status of the GPRS Tunneling Protocol (GTP) on the GGSN (such as activated PDP contexts, throughput, and QoS statistics), use the **show gprs gtp status** privileged EXEC command.

**show gprs gtp status**

---

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

## subscription-required

To specify that a subscription is required to access a PDN through a particular access point, use the **subscription-required** access-point configuration command. To restore the default setting (no subscription is required), use the **no** form of the command.

**subscription-required**

**no subscription-required**

---

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

## use-interface

To configure the GGSN to use a specific interface for user access at a particular access point, use the **use-interface** access-point configuration command. To deactivate the use of a specific interface, use the **no** form of the command.

**use-interface** *interface\_name* **next-hop-address** *ip\_address*

**no use-interface** *interface\_name* **next-hop-address** *ip\_address*

---

<b>Syntax Description</b>	<i>interface_name</i>	Name of an interface on the router to be used by the specified access point.
	<i>ip_address</i>	IP address of the gateway device for the virtual private network.

---



## SGSN D-Node Commands

---

This chapter describes the function and syntax of the SGDN D-Node commands. The commands in this section are for certain operator-specific, SGSN D-node implementations only. These commands are not to be used for any other type of standard, SGSN-related configuration, or to configure any GGSN services. For more information about these commands, refer to the appendix in the *Cisco IOS Mobile Wireless Command Reference*.

### clear gprs isgsn statistics

To clear the current GPRS intra-Serving GPRS Support Node (iSGSN) statistics, use the **clear gprs isgsn statistics** privileged EXEC command (SGSN D-node only).

```
clear gprs isgsn statistics
```

---

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

### clear l2relay statistics

To clear the Layer 2 Relay (l2relay) statistics for the SGSN, use the **clear l2relay statistics** privileged EXEC command (SGSN D-node only).

```
clear l2relay statistics
```

---

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

## clear l2relay topology-map

To clear the Layer 2 Relay topology map for the SGSN, use the **clear l2relay topology-map** privileged EXEC command (SGSN D-node only).

**clear l2relay topology-map**

---

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

## l2relay echo-interval

To specify the interval at which the SGSN sends l2relay keepalive messages, use the **l2relay echo-interval** global configuration command. To restore the default value for the echo interval (10 seconds) use the **no** form of the command (SGSN D-node only).

**l2relay echo-interval** *seconds*

**no l2relay echo-interval**

---

**Syntax Description**

<i>seconds</i>	The length of the echo interval, in seconds. Specify a value between 1 and 360 seconds. The default is 10 seconds.
----------------	--

---

## l2relay flow-control

To specify quench threshold and resume threshold percentages that determine when the l2relay protocol begins and ends flow control processing, use the **l2relay flow-control** global configuration command. To restore the default values for flow control processing, use the **no** form of the command (SGSN D-node only).

**l2relay flow-control** { **enable** | *quench-threshold* | *resume-threshold* }

**no l2relay flow-control**

---

**Syntax Description**

<b>enable</b>	Enables flow control.
<i>quench-threshold</i>	The percentage of congestion that triggers flow control processing.
<i>resume-threshold</i>	The percentage of congestion that triggers resumption of normal processing.

---

## l2relay pilot-uid

To specify the unit ID of an SGSN-T node to which packets with unknown destination information are transmitted, use the **l2relay pilot-uid** global configuration command. To delete the pilot UID, use the **no** form of the command (SGSN D-node only).

**l2relay pilot-uid** *uid*

**no l2relay pilot-uid**

<b>Syntax Description</b>	<i>uid</i>	Number between 1 and 32 that specifies unit ID for the pilot unit. The default is 0xFF.
---------------------------	------------	---

## l2relay use-interface

To specify the physical interfaces used by the l2relay protocol running on the SGSN, use the **l2relay use-interface** global configuration command (SGSN D-node only).

**l2relay use-interface** *interface\_1* [*interface\_2*]

<b>Syntax Description</b>	<i>interface_1</i>	Interface that is used by the Layer 2 Relay protocol.
	<i>interface_2</i>	A secondary interface that can be used by the Layer 2 Relay protocol.

## show gprs isgsn statistics

To display statistics that show the status of the intra-Serving GPRS Support Node running on the router, use the **show gprs isgsn statistics** privileged EXEC command (SGSN D-node only).

**show gprs isgsn statistics**

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

## show l2relay statistics

To display statistics that show the status of the Layer 2 Relay Protocol running on the SGSN, use the **show l2relay statistics** privileged EXEC command (SGSN D-node only).

**show l2relay statistics**

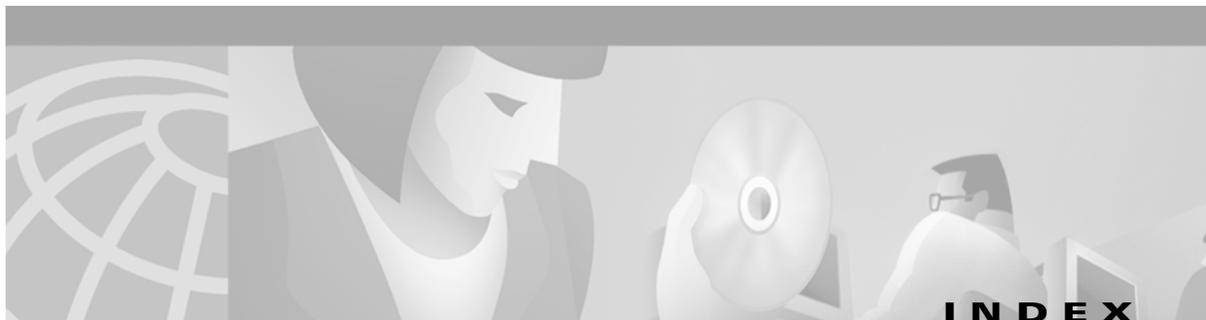
<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--

■ show l2relay statistics



## **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

---

## Symbols

? command **xvi**

---

## A

access-expression command **CS3-27**

access-list command **CS3-27**

access-list (extended-ibm) command **CS3-3**

access-list rate-limit command **CS3-277**

access-list (standard-ibm) command **CS3-4**

access-list (type-code-ibm) command **CS3-4**

access-mode command **CS3-569**

access-point command **CS3-569**

access-point-name command **CS3-570**

access-violation command **CS3-570**

acc-qos command **CS3-343**

adapter command **CS3-229**

alias static command **CS3-344**

allocate lu command **CS3-251**

alps a1-map a2-map command **CS3-151**

alps alias command **CS3-152**

alps ascu command **CS3-152**

alps auto-reset command **CS3-152**

alps circuit command **CS3-153**

alps connection-type permanent command **CS3-153**

alps default-circuit command **CS3-153**

alps enable-alarms ascu command **CS3-154**

alps enable-alarms circuit command **CS3-154**

alps enable-alarms peer command **CS3-154**

alps enable-ascu command **CS3-155**

alps enable-circuit command **CS3-155**

alps error-display command **CS3-155**

alps host-hld host-link command **CS3-156**

alps hostlink command **CS3-156**

alps idle-timer command **CS3-157**

alps keepalive command **CS3-157**

alps lifetime-timer command **CS3-158**

alps local-hld remote-hld command **CS3-158**

alps local-peer command **CS3-158**

alps matip-close-delay command **CS3-159**

alps max-msg-length command **CS3-159**

alps mpx command **CS3-159**

alps n1 command **CS3-160**

alps n2 command **CS3-160**

alps n3 command **CS3-160**

alps poll-pause command **CS3-161**

alps primary-peer command **CS3-161**

alps remote-peer command **CS3-161**

alps retry-option command **CS3-162**

alps service-msg data-drop command **CS3-164**

alps service-msg format command **CS3-164**  
 alps service-msg status-change command **CS3-164**  
 alps service-msg-interval command **CS3-163**  
 alps service-msg-list command **CS3-163**  
 alps service-msg-list number command **CS3-163**  
 alps servlim command **CS3-165**  
 alps t1 command **CS3-165**  
 alps t2 command **CS3-165**  
 alps translate command **CS3-166**  
 alps update-circuit command **CS3-166**  
 alt-dial command **CS3-345**  
 answer-address command **CS3-345**  
 application command **CS3-345**  
 arq reject-unknown-prefix command **CS3-346**  
 asp addr-offset command **CS3-95**  
 asp role command **CS3-95**  
 asp rx-ift command **CS3-96**  
 atm compression command **CS3-346**  
 atm scramble-enable command **CS3-346**  
 atm video aesa command **CS3-347**  
 audio-prompt load command **CS3-347**  
 auto-cut-through command **CS3-347**

---

## B

bandwidth command **CS3-348**  
 bandwidth (policy-map class) command **CS3-278**  
 bandwidth remote command **CS3-348**  
 battery-reversal command **CS3-348**  
 bgp-policy command **CS3-278**  
 block-caller command **CS3-349**  
 bridge acquire command **CS3-5**  
 bridge address command **CS3-5**  
 bridge bitswap-layer3-addresses command **CS3-6**  
 bridge bridge command **CS3-6**  
 bridge circuit-group pause command **CS3-6**  
 bridge circuit-group source-based command **CS3-7**  
 bridge cmf command **CS3-7**  
 bridge crb command **CS3-7**  
 bridge domain command **CS3-8**  
 bridge forward-time command **CS3-8**  
 bridge hello-time command **CS3-16**  
 bridge irb command **CS3-16**  
 bridge lat-service-filtering command **CS3-17**  
 bridge max-age command **CS3-17**  
 bridge multicast-source command **CS3-17**  
 bridge priority command **CS3-18**  
 bridge protocol command **CS3-18**  
 bridge protocol ibm command **CS3-28**  
 bridge route command **CS3-18**  
 bridge subscriber-policy command **CS3-19**  
 bridge-group aging-time command **CS3-9**  
 bridge-group cbus-bridging command **CS3-9**  
 bridge-group circuit-group command **CS3-9**  
 bridge-group command **CS3-8**  
 bridge-group input-address-list command **CS3-10**  
 bridge-group input-lat-service-deny command **CS3-10**  
 bridge-group input-lat-service-permit command **CS3-10**  
 bridge-group input-lsap-list command **CS3-11**  
 bridge-group input-pattern-list command **CS3-11**  
 bridge-group input-type-list command **CS3-11**  
 bridge-group lat-compression command **CS3-12**  
 bridge-group output-address-list command **CS3-12**  
 bridge-group output-lat-service-deny command **CS3-12**  
 bridge-group output-lat-service-permit command **CS3-13**  
 bridge-group output-lsap-list command **CS3-13**  
 bridge-group output-pattern-list command **CS3-13**  
 bridge-group output-type-list command **CS3-14**  
 bridge-group path-cost command **CS3-14**  
 bridge-group priority command **CS3-14**  
 bridge-group spanning-disabled command **CS3-15**  
 bridge-group sse command **CS3-15**  
 bridge-group subscriber-loop-control command **CS3-15**  
 bridge-group subscriber-trunk command **CS3-16**  
 bsc char-set command **CS3-96**  
 bsc contention command **CS3-96**  
 bsc dial-contention command **CS3-97**  
 bsc host-timeout command **CS3-97**

bsc pause command **CS3-97**  
 bsc poll-timeout command **CS3-98**  
 bsc primary command **CS3-98**  
 bsc retries command **CS3-98**  
 bsc secondary command **CS3-99**  
 bsc servlim command **CS3-99**  
 bsc spec-poll command **CS3-99**  
 bsc-char-set command **CS3-96**  
 bstun group command **CS3-100**  
 bstun keepalive-count command **CS3-100**  
 bstun lisnsap command **CS3-100**  
 bstun peer-name command **CS3-101**  
 bstun protocol-group command **CS3-101**  
 bstun remote-peer-keepalive command **CS3-102**  
 bstun route command **CS3-102**  
 bstun route (Frame Relay) command **CS3-102**  
 bump command **CS3-278**  
 bundle command **CS3-279**  
 busyout forced command **CS3-349**  
 busyout monitor interface command **CS3-349**  
 busyout monitor probe command **CS3-350**  
 busyout seize command **CS3-351**

---

## C

cac master command **CS3-352**  
 cadence-list command **CS3-352**  
 cadence-max-off-time command **CS3-353**  
 cadence-min-on-time command **CS3-353**  
 cadence-variation command **CS3-353**  
 call application voice command **CS3-354**  
 call application voice language command **CS3-357**  
 call application voice pin-len command **CS3-358**  
 call application voice redirect-number command **CS3-358**  
 call application voice retry-count command **CS3-358**  
 call application voice set-location command **CS3-359**  
 call application voice uid-len command **CS3-359**  
 call application voice warning-time command **CS3-360**  
 call rsvp-sync resv-timer command **CS3-365**  
 call start command **CS3-365**  
 caller-id alerting dsp-pre-alloc command **CS3-366**  
 caller-id alerting line-reversal command **CS3-367**  
 caller-id alerting pre-ring command **CS3-367**  
 caller-id alerting ring command **CS3-367**  
 caller-id attenuation command **CS3-368**  
 caller-id block command **CS3-368**  
 caller-id enable command **CS3-368**  
 call-waiting command **CS3-365**  
 cap-list vfc command **CS3-369**  
 ccs connect (controller) command **CS3-370**  
 ccs encaps frf11 command **CS3-371**  
 certificate reload command **CS3-251**  
 ces cell-loss-integration-period command **CS3-371**  
 ces clockmode synchronous command **CS3-372**  
 ces connect command **CS3-372**  
 ces initial-delay command **CS3-373**  
 ces max-buf-size command **CS3-373**  
 ces service command **CS3-373**  
 ces-clock command **CS3-371**  
 channel-protocol command **CS3-229**  
 class (policy-map) command **CS3-279**  
 class-bundle command **CS3-280**  
 class-map command **CS3-280**  
 claw (backup) command **CS3-240**  
 claw command **CS3-239**  
 clear alps circuits command **CS3-166**  
 clear alps counters command **CS3-166**  
 clear bridge command **CS3-19**  
 clear bridge multicast command **CS3-19**  
 clear call fallback cache command **CS3-374**  
 clear call fallback stats command **CS3-374**  
 clear csm-statistics command **CS3-374, CS3-375**  
 clear dbconn connection command **CS3-213**  
 clear dbconn statistic command **CS3-213**  
 clear dlsw circuit command **CS3-67**  
 clear dlsw reachability command **CS3-67**  
 clear dlsw statistics command **CS3-67**  
 clear drip counters command **CS3-55, CS3-57**

- clear extended counters command **CS3-230**
  - clear gprs charging cdr command **CS3-570**
  - clear gprs gtp pdp-context command **CS3-571**
  - clear gprs gtp statistics command **CS3-571**
  - clear gprs isgsn statistics command **CS3-589**
  - clear h323 gatekeeper call command **CS3-375**
  - clear l2relay statistics command **CS3-589**
  - clear l2relay topology-map command **CS3-590**
  - clear mgcp statistics command **CS3-375**
  - clear ncia circuit command **CS3-147**
  - clear ncia client command **CS3-147**
  - clear ncia client registered command **CS3-147**
  - clear netbios-cache command **CS3-28**
  - clear rif-cache command **CS3-29**
  - clear sgcp statistics command **CS3-376**
  - clear source-bridge command **CS3-29**
  - clear sse command **CS3-29**
  - clear txconn connection command **CS3-214**
  - clear txconn statistic command **CS3-214**
  - clear txconn transaction command **CS3-213**
  - clear vlan statistics command **CS3-20**
  - clear voice port command **CS3-376**
  - client ip command **CS3-252**
  - client ip lu command **CS3-252**
  - client ip pool command **CS3-253**
  - client lu maximum command **CS3-253**
  - client pool command **CS3-253**
  - clock rate line command **CS3-376**
  - clock rate network-clock command **CS3-376**
  - clock-select command **CS3-377**
  - cmpe command **CS3-245**
  - codec aal2-profile command **CS3-381**
  - codec complexity command **CS3-381**
  - codec (dial-peer) command **CS3-377**
  - codec (dsp) command **CS3-380**
  - codec preference command **CS3-382**
  - codec (voice-port) command
    - See* codec (dial-peer) command
  - comfort-noise command **CS3-383**
  - command modes, understanding **xv to xvi**
  - command syntax
    - conventions **x**
    - displaying (example) **xvii**
  - commands
    - context-sensitive help for abbreviating **xvi**
    - default form, using **xix**
    - no form, using **xix**
  - compand-type command **CS3-384**
  - condition command **CS3-384**
  - connect (atm) command **CS3-385**
  - connect command **CS3-385**
  - connect (global) command **CS3-386**
  - connect voice command **CS3-386**
  - connection command **CS3-386**
  - connection-timeout command **CS3-387**
  - copy flash vfc command **CS3-387**
  - copy tftp vfc command **CS3-387**
  - eptone command **CS3-388**
  - cross-connect command **CS3-390**
  - csna command **CS3-245**
  - customer-id command **CS3-391**
  - custom-queue-list command **CS3-280**
- 
- D**
- dbconn license command **CS3-215**
  - dbconn pem command **CS3-215**
  - dbconn ping command **CS3-216**
  - dbconn server command **CS3-216**
  - dbconn tcpserver command **CS3-218**
  - debug dbconn command **CS3-219**
  - default command **CS3-393**
  - default-file vfc command **CS3-394**
  - default-profile command **CS3-254**
  - define command **CS3-394**
  - delete vfc command **CS3-394**
  - description command **CS3-395**
  - description (dspfarm) command **CS3-395**

- destination-pattern command **CS3-395**
- destination-pattern (ISDN) command **CS3-396**
- detect v54 channel-group command **CS3-397**
- device-id command **CS3-397**
- dhcp-gateway-address command **CS3-571**
- dhcp-server command **CS3-572**
- dial-control-mib command **CS3-397**
- dial-peer configuration command **CS3-366**
- dial-peer hunt command **CS3-397**
- dial-peer terminator command **CS3-398**
- dial-peer video command **CS3-398**
- dial-peer voice command **CS3-399**
- dial-type command **CS3-400**
- digit-strip command **CS3-400**
- direct-inward-dial command **CS3-400**
- disable (TN3270) command **CS3-255**
- disc\_pi\_off command **CS3-401**
- disconnect qdm command **CS3-280**
- disconnect-ack command **CS3-401**
- dlsw allroute-netbios command **CS3-68**
- dlsw allroute-sna command **CS3-68**
- dlsw bgroup-list command **CS3-68**
- dlsw bridge-group command **CS3-69**
- dlsw cache-ignore-netbios-datagram command **CS3-70**
- dlsw disable command **CS3-70**
- dlsw duplicate-path-bias command **CS3-70, CS3-71**
- dlsw explorerq-depth command **CS3-71**
- dlsw group-cache disable command **CS3-71**
- dlsw group-cache max entries command **CS3-71**
- dlsw icannotreach saps command **CS3-72**
- dlsw icanreach command **CS3-72**
- dlsw llc2 nornr command **CS3-73**
- dlsw load-balance command **CS3-73**
- dlsw local-peer command **CS3-73**
- dlsw mac-addr command **CS3-74**
- dlsw max-multiple-rifs command **CS3-75**
- dlsw netbios-keepalive-filter command **CS3-75**
- dlsw netbios-name command **CS3-75**
- dlsw peer-on-demand-defaults command **CS3-76**
- dlsw port-list command **CS3-77**
- dlsw prom-peer-defaults command **CS3-78**
- dlsw redundant-rings command **CS3-79**
- dlsw remote-peer frame relay command **CS3-79**
- dlsw remote-peer fst command **CS3-81**
- dlsw remote-peer interface command **CS3-82**
- dlsw remote-peer tcp command **CS3-83**
- dlsw ring-list command **CS3-85**
- dlsw rsvp command **CS3-86**
- dlsw timer command **CS3-86**
- dlsw tos disable command **CS3-87**
- dlsw tos map command **CS3-88**
- dlsw transparent map command **CS3-88**
- dlsw transparent redundancy-enable command **CS3-88**
- dlsw transparent switch-support command **CS3-89**
- dlsw transparent timers command **CS3-89**
- dlsw udp-disable command **CS3-87, CS3-88, CS3-89**
- dlur command **CS3-255**
- dlus-backup command **CS3-255**
- domain-id command **CS3-256**
- ds0 busyout command **CS3-401**
- ds0-group command **CS3-402, CS3-472**
- dscp command **CS3-281**
- dsn command **CS3-408**
- dspint dspfarm command **CS3-409**
- dspu activation-window command **CS3-171**
- dspu default-pu command **CS3-171**
- dspu enable-host (QLLC) command **CS3-172**
- dspu enable-host (SDLC) command **CS3-172**
- dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay) command **CS3-172**
- dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI) command **CS3-173**
- dspu enable-pu (QLLC) command **CS3-173**
- dspu enable-pu (SDLC) command **CS3-173**
- dspu host (Frame Relay) command **CS3-174**
- dspu host (QLLC) command **CS3-175**
- dspu host (SDLC) command **CS3-175**
- dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC) command **CS3-176**

dspu lu command **CS3-177**  
 dspu ncia command **CS3-177**  
 dspu ncia enable-pu command **CS3-178**  
 dspu notification-level command **CS3-178**  
 dspu pool command **CS3-178**  
 dspu pu (Frame Relay) command **CS3-179**  
 dspu pu (QLLC) command **CS3-179**  
 dspu pu (SDLC) command **CS3-180**  
 dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA) command **CS3-181**  
 dspu rsrb command **CS3-181**  
 dspu rsrb enable-host command **CS3-182**  
 dspu rsrb enable-pu command **CS3-182**  
 dspu rsrb start command **CS3-182**  
 dspu start command **CS3-183**  
 dspu vdlc command **CS3-183**  
 dspu vdlc enable-host command **CS3-183**  
 dspu vdlc enable-pu command **CS3-184**  
 dspu vdlc start command **CS3-184**  
 dtmf-relay (Voice over Frame Relay) command **CS3-410**  
 dtmf-relay (Voice over IP) command **CS3-409**  
 dtmf-timer-inter-digit command **CS3-410**

---

## E

echo-cancel comfort-noise command **CS3-410**  
 echo-cancel compensation command **CS3-411**  
 echo-cancel coverage command **CS3-411**  
 echo-cancel enable command **CS3-411**  
 echo-cancel enable (controller) command **CS3-412**  
 echo-cancel loopback command **CS3-412**  
 enable (TN3270) command **CS3-256**  
 enabling security, TN3270 server **CS3-256, CS3-266**  
 encapsulation alc command **CS3-167**  
 encapsulation atm-ces command **CS3-413**  
 encapsulation bstun command **CS3-103**  
 encapsulation command **CS3-412**  
 encapsulation ftc-trunk command **CS3-413**  
 encapsulation gtp command **CS3-572**

encapsulation sdlc command **CS3-115**  
 encapsulation sdlc-primary command **CS3-115**  
 encapsulation sdlc-secondary command **CS3-116**  
 encapsulation stun command **CS3-103**  
 encapsulation tr-isl command **CS3-55**  
 encapsulation uts command **CS3-167**  
 encryption command **CS3-413**  
 encryptorder command **CS3-256**  
 erase vfc command **CS3-414**  
 ethernet-transit-oui command **CS3-29**  
 exception slot command **CS3-230**  
 expect-factor command **CS3-414**  
 exponential-weighting-constant command **CS3-281**

---

## F

fair-queue aggregate-limit command **CS3-283**  
 fair-queue (class-default) command **CS3-282**  
 fair-queue (DWFQ) command **CS3-282**  
 fair-queue individual-limit command **CS3-284**  
 fair-queue limit command **CS3-284**  
 fair-queue (policy-map) command **CS3-282**  
 fair-queue qos-group command **CS3-284**  
 fair-queue tos command **CS3-285**  
 fair-queue weight command **CS3-285**  
 fair-queue (WFQ) command **CS3-283**  
 fax protocol (dial-peer) command **CS3-414**  
 fax protocol (voice-service) command **CS3-415**  
 fax rate command **CS3-415**  
 fax receive called-subscriber command **CS3-416**  
 fax send center-header command **CS3-416**  
 fax send coveragepage comment command **CS3-417**  
 fax send coveragepage e-mail-controllable command **CS3-417**  
 fax send coveragepage enable command **CS3-418**  
 fax send coveragepage show-detail command **CS3-418**  
 fax send left-header command **CS3-418**  
 fax send max-speed command **CS3-419**  
 fax send right-header command **CS3-419**

fax send transmitting-subscriber command **CS3-419**  
 fax-relay ecm disable command **CS3-416**  
 filtering output, show and more commands **xx**  
 forward-digits command **CS3-420**  
 frame-relay interface-queue priority command **CS3-285**  
 frame-relay ip rtp priority command **CS3-286**  
 frame-relay map bridge broadcast command **CS3-20**  
 frame-relay map bstun command **CS3-104**  
 frame-relay map llc2 command **CS3-141**  
 frame-relay map rsrb command **CS3-141**  
 frame-relay voice bandwidth command **CS3-420**  
 fras backup dlsw command **CS3-142**  
 fras ban command **CS3-142**  
 fras ddr-backup command **CS3-143**  
 fras map llc command **CS3-144**  
 fras map sdhc command **CS3-144**  
 fras-host ban command **CS3-143**  
 fras-host bnn command **CS3-143**  
 fras-host dlsw-local-ack command **CS3-144**  
 freq-max-delay command **CS3-421**  
 freq-max-deviation command **CS3-421**  
 freq-max-power command **CS3-422**  
 freq-min-power command **CS3-422**  
 freq-pair command **CS3-422**  
 freq-power-twist command **CS3-423**

---

## G

gatekeeper command **CS3-425**  
 gateway command **CS3-425**  
 generic-pool command **CS3-257**  
 gprs access-point-list command **CS3-572**  
 gprs canonical-qos best-effort bandwidth-factor  
 command **CS3-573**  
 gprs canonical-qos gsn-resource-factor  
 command **CS3-573**  
 gprs canonical-qos map tos command **CS3-573**  
 gprs canonical-qos premium mean-throughput-deviation  
 command **CS3-574**

gprs charging cdr-aggregation-limit command **CS3-574**  
 gprs charging cdr-option local-record-sequence-number  
 command **CS3-574**  
 gprs charging cdr-option node-id command **CS3-575**  
 gprs charging cg-path-requests command **CS3-575**  
 gprs charging container volume-threshold  
 command **CS3-575**  
 gprs charging disable command **CS3-576**  
 gprs charging flow-control private-echo  
 command **CS3-576**  
 gprs charging map data tos command **CS3-576**  
 gprs charging packet-queue-size command **CS3-577**  
 gprs charging path-protocol command **CS3-577**  
 gprs charging server-switch-timer command **CS3-577**  
 gprs charging tariff-time command **CS3-578**  
 gprs charging transfer interval command **CS3-578**  
 gprs default charging-gateway command **CS3-578**  
 gprs default dhcp-server command **CS3-579**  
 gprs default ip-address-pool command **CS3-579**  
 gprs default radius-server command **CS3-579**  
 gprs fastswitch command **CS3-580**  
 gprs gtp error-indication throttle command **CS3-580**  
 gprs gtp map signalling tos command **CS3-580**  
 gprs gtp n3-buffer-size command **CS3-581**  
 gprs gtp n3-requests command **CS3-581**  
 gprs gtp path-echo-interval command **CS3-581**  
 gprs gtp t3-response command **CS3-582**  
 gprs gtp t3-tunnel command **CS3-582**  
 gprs idle-pdp-context purge-timer command **CS3-582**  
 gprs maximum-pdp-context-allowed command **CS3-583**  
 gprs qos default-response requested command **CS3-583**  
 gprs qos map canonical-qos command **CS3-583**  
 gprs radius msisdn first-byte command **CS3-584**  
 group codes, access to  
     denying **CS3-10, CS3-12**  
     permitting **CS3-10, CS3-13**  
 gw-accounting command **CS3-426**  
 gw-type-prefix command **CS3-426**

**H**

h225 timeout tcp establish command **CS3-427**  
h323 asr bandwidth command **CS3-427**  
h323 call start command **CS3-427**  
h323 gatekeeper command **CS3-428**  
h323 h323-id command **CS3-430**  
h323 interface command **CS3-430**  
h323 qos command **CS3-431**  
h323 t120 command **CS3-431**  
h323-gateway voip bind srcaddr command **CS3-428**  
h323-gateway voip h323-id command **CS3-428**  
h323-gateway voip id command **CS3-429**  
h323-gateway voip tech-prefix command **CS3-430**  
help command **xvi**  
huntstop command **CS3-431**

**I**

icpif command **CS3-432**  
idle-time command **CS3-257**  
idle-voltage command **CS3-432**  
ignore command **CS3-432**  
image resolution command **CS3-433**  
imaging encoding command **CS3-433**  
impedance command **CS3-433**  
incoming called-number command **CS3-434**  
information-type command **CS3-434**  
input gain command **CS3-434**  
interface bvi command **CS3-20**  
interface channel command **CS3-231**  
interface virtual-tokenring command **CS3-145**  
interface vlan command **CS3-57**  
ip nbar protocol-discovery command **CS3-287**  
ip precedence command **CS3-257**  
ip precedence (dial-peer) command **CS3-435**  
ip rsvp atm-peak-rate-limit command **CS3-288**  
ip rsvp bandwidth command **CS3-288**  
ip rsvp burst policing command **CS3-288**  
ip rsvp dsbm candidate command **CS3-289**  
ip rsvp dsbm non-resv-send-limit command **CS3-289**  
ip rsvp flow-assist command **CS3-290**  
ip rsvp neighbor command **CS3-290**  
ip rsvp policy cops minimal command **CS3-290**  
ip rsvp policy cops report-all command **CS3-291**  
ip rsvp policy cops servers command **CS3-291**  
ip rsvp policy cops timeout command **CS3-291**  
ip rsvp policy default-reject command **CS3-292**  
ip rsvp pq-profile command **CS3-292**  
ip rsvp precedence command **CS3-293**  
ip rsvp reservation command **CS3-293**  
ip rsvp reservation-host command **CS3-294**  
ip rsvp sender command **CS3-295**  
ip rsvp sender-host command **CS3-296**  
ip rsvp signalling dscp command **CS3-296**  
ip rsvp svc-required command **CS3-297**  
ip rsvp tos command **CS3-297**  
ip rsvp udp-multicasts command **CS3-298**  
ip rtp priority command **CS3-298**  
ip tos command **CS3-258**  
ip udp checksum command **CS3-435**  
ip-access-group command **CS3-584**  
ip-address-pool command **CS3-584**  
isdn contiguous-bchan command **CS3-435**  
isdn global-disconnect command **CS3-436**  
isdn i-number command **CS3-436**  
isdn network-failure-cause command **CS3-436**  
ivr autoloading command **CS3-438**  
ivr autoloading mode command **CS3-439**  
ivr autoloading retry command **CS3-438**  
ivr prompt memory command **CS3-439**

**K**

keepalive (TN3270) command **CS3-258**  
keylen command **CS3-259**

**L**

l2relay echo-interval command **CS3-590**  
 l2relay flow-control command **CS3-590**  
 l2relay pilot-uid command **CS3-591**  
 l2relay use-interface command **CS3-591**  
 lan command **CS3-231**  
 lan-name command **CS3-184**  
 line-power command **CS3-440**  
 link (TN3270) command **CS3-259**  
 listen-point command **CS3-259**  
 llc2 ack-delay-time command **CS3-116**  
 llc2 ack-max command **CS3-116**  
 llc2 dynwind command **CS3-145**  
 llc2 idle-time command **CS3-117**  
 llc2 local-window command **CS3-117**  
 llc2 n1 command **CS3-117**  
 llc2 n2 command **CS3-118**  
 llc2 nw command **CS3-118**  
 llc2 recv-window command **CS3-118**  
 llc2 send-window command **CS3-119**  
 llc2 t1-time command **CS3-119**  
 llc2 tbusy-time command **CS3-119**  
 llc2 tpf-time command **CS3-120**  
 llc2 trej-time command **CS3-120**  
 llc2 xid-neg-val-time command **CS3-120**  
 llc2 xid-retry-time command **CS3-121**  
 lnm alternate command **CS3-30**  
 lnm crs command **CS3-30**  
 lnm disabled command **CS3-30**  
 lnm express-buffer command **CS3-31**  
 lnm loss-threshold command **CS3-31**  
 lnm password command **CS3-31**  
 lnm pathtrace-disabled command **CS3-32**  
 lnm rem command **CS3-32**  
 lnm rps command **CS3-32**  
 lnm snmp-only command **CS3-32**  
 lnm softerr command **CS3-33**  
 locaddr-priority command **CS3-59**

locaddr-priority-list command **CS3-59**  
 loopback (T1 controller) command **CS3-440**  
 loop-detect command **CS3-441**  
 loss-plan command **CS3-441**  
 lrq forward-queries command **CS3-442**  
 lrq reject-unknown-prefix command **CS3-442**  
 lrq timeout blast window command **CS3-442**  
 lrq timeout seq delay command **CS3-443**  
 lsap command **CS3-260**  
 lu deletion command **CS3-260**  
 lu termination command **CS3-261**

**M**

mac-address command **CS3-33**  
 match access-group command **CS3-298**  
 match any command **CS3-299**  
 match class-map command **CS3-299**  
 match cos command **CS3-299**  
 match destination-address mac command **CS3-300**  
 match input-interface command **CS3-300**  
 match ip dscp command **CS3-300**  
 match ip precedence command **CS3-301**  
 match ip rtp command **CS3-301**  
 match mpls experimental command **CS3-302**  
 match not command **CS3-302**  
 match protocol citrix command **CS3-303**  
 match protocol command **CS3-302**  
 match protocol http command **CS3-304**  
 match qos-group command **CS3-304**  
 match source-address mac command **CS3-305**  
 max-connection command **CS3-443**  
 max-forwards command **CS3-444**  
 maximum-lus command **CS3-261**  
 max-llc2-sessions command **CS3-231**  
 max-redirects command **CS3-444**  
 max-reserved-bandwidth command **CS3-305**  
 mdn command **CS3-444**  
 mgcp block-newcalls command **CS3-445**

mgcp call-agent command **CS3-445**  
 mgcp codec command **CS3-445**  
 mgcp command **CS3-444**  
 mgcp default-package command **CS3-446**  
 mgcp dtmf-relay command **CS3-446**  
 mgcp ip-tos command **CS3-447**  
 mgcp max-waiting-delay command **CS3-447**  
 mgcp modem passthru command **CS3-447**  
 mgcp package-capability command **CS3-448**  
 mgcp playout command **CS3-449**  
 mgcp quality-threshold command **CS3-449**  
 mgcp request retries command **CS3-450**  
 mgcp request timeout command **CS3-450**  
 mgcp restart-delay command **CS3-450**  
 mgcp sdp simple command **CS3-451**  
 mgcp vad command **CS3-451**  
 microcode reload controller command **CS3-451**  
 mmoip aaa global-password command **CS3-451**  
 mmoip aaa method fax accounting command **CS3-452**  
 mmoip aaa method fax authentication command **CS3-452**  
 mmoip aaa receive-accounting enable command **CS3-452**  
 mmoip aaa receive-authentication enable  
 command **CS3-453**  
 mmoip aaa receive-id primary command **CS3-453**  
 mmoip aaa receive-id secondary command **CS3-453**  
 mmoip aaa send-accounting enable command **CS3-454**  
 mmoip aaa send-authentication enable command **CS3-454**  
 mmoip aaa send-id primary command **CS3-454**  
 mmoip aaa send-id secondary command **CS3-455**  
 mode ccs command **CS3-456**  
 mode (Voice over ATM) command **CS3-455**  
 modem passthrough (dial-peer) command **CS3-456**  
 modem passthrough (voice-service) command **CS3-457**  
 mta receive aliases command **CS3-457**  
 mta receive generate-mdn command **CS3-458**  
 mta receive maximum-recipients command **CS3-458**  
 mta send mail-from command **CS3-458**  
 mta send origin-prefix command **CS3-459**  
 mta send postmaster command **CS3-459**

mta send return-receipt-to command **CS3-459**  
 mta send server command **CS3-460**  
 mta send subject command **CS3-460**  
 multiring command **CS3-33**  
 multiring trcrf-vlan command **CS3-56, CS3-58**  
 music-threshold command **CS3-460**

---

## N

name command **CS3-232**  
 ncia client command **CS3-148**  
 ncia command **CS3-148**  
 ncia rsrc command **CS3-148**  
 ncia server command **CS3-149**  
 netbios access-list bytes command **CS3-34**  
 netbios access-list host command **CS3-34**  
 netbios enable-name-cache command **CS3-35**  
 netbios input-access-filter bytes command **CS3-35**  
 netbios input-access-filter host command **CS3-35**  
 netbios name-cache command **CS3-36**  
 netbios name-cache name-len command **CS3-36**  
 netbios name-cache proxy-datagram command **CS3-36**  
 netbios name-cache query-timeout command **CS3-37**  
 netbios name-cache recognized-timeout  
 command **CS3-37**  
 netbios name-cache timeout command **CS3-37**  
 netbios output-access-filter bytes command **CS3-38**  
 netbios output-access-filter host command **CS3-38**  
 network-clock base-rate command **CS3-460**  
 network-clock-switch command **CS3-461**  
 new information in this release **ix**  
 non-linear command **CS3-461**  
 nsap command **CS3-461**  
 numbering-type command **CS3-462**  
 num-exp command **CS3-462**

---

## O

oam-bundle command **CS3-305**

offload alias command **CS3-242**  
 offload (backup) command **CS3-242**  
 offload command **CS3-241**  
 operation command **CS3-462**  
 output attenuation command **CS3-463**

---

## P

path command **CS3-243**  
 ping sna command **CS3-193**  
 playout-delay command **CS3-463, CS3-464**  
 playout-delay mode command **CS3-465**  
 police command **CS3-306**  
 policy-map command **CS3-306**  
 pool command **CS3-261**  
 port media command **CS3-467**  
 port signal command **CS3-467**  
 port (voice) command **CS3-465**  
 pots call-waiting command **CS3-468**  
 pots dialing-method command **CS3-468**  
 pots disconnect-time command **CS3-469**  
 pots distinctive-ring-guard-time command **CS3-469**  
 pots encoding command **CS3-470**  
 pots line-type command **CS3-470**  
 pots ringing-freq command **CS3-470**  
 precedence (VC bundle) command **CS3-307**  
 precedence (WRED group) command **CS3-307**  
 pre-dial delay command **CS3-471**  
 preference command **CS3-472**  
 preferred-nnserver command **CS3-262**  
 prefix command **CS3-472**  
 pri-group command **CS3-472**  
 pri-group nec-fusion command **CS3-473**  
 priority command **CS3-308**  
 priority-group command **CS3-308**  
 priority-list command **CS3-60**  
 priority-list default command **CS3-308**  
 priority-list interface command **CS3-309**  
 priority-list protocol bstun command **CS3-104**

priority-list protocol command **CS3-309**  
 priority-list protocol ip tcp command **CS3-104**  
 priority-list queue-limit command **CS3-310**  
 priority-list stun address command **CS3-105**  
 profile command **CS3-262**  
 progress\_ind command **CS3-473**  
 protect command **CS3-310**  
 protocol-type command **CS3-585**  
 proxy h323 command **CS3-474**  
 pu (DLUR) command **CS3-263**  
 pu dlur (listen-point) command **CS3-265**  
 pu (listen-point) command **CS3-263**  
 pu (TN3270) command **CS3-264**  
 pvc-bundle command **CS3-310**

---

## Q

qllc accept-all-calls command **CS3-131**  
 qllc dlsw command **CS3-90**  
 qllc largest-packet command **CS3-131**  
 qllc npsi-poll command **CS3-132**  
 qllc partner command **CS3-132**  
 qllc sap command **CS3-132**  
 qllc srb command **CS3-133**  
 qllc xid command **CS3-133**  
 qos pre-classify command **CS3-311**  
 question mark (?) command **xvi**  
 queue-limit command **CS3-311**  
 queue-list default command **CS3-312**  
 queue-list interface command **CS3-312**  
 queue-list protocol bstun command **CS3-106**  
 queue-list protocol command **CS3-312**  
 queue-list protocol ip tcp command **CS3-106**  
 queue-list queue byte-count command **CS3-313**  
 queue-list queue limit command **CS3-313**

**R**

radius-server command **CS3-585**  
 random-detect dscp command **CS3-313**  
 random-detect exponential-weighting-constant  
 command **CS3-315**  
 random-detect flow average-depth-factor  
 command **CS3-316**  
 random-detect flow command **CS3-315**  
 random-detect flow count command **CS3-316**  
 random-detect (interface) command **CS3-314**  
 random-detect (per VC) command **CS3-315**  
 random-detect precedence command **CS3-317**  
 random-detect-group command **CS3-316**  
 rate-limit command **CS3-317**  
 register command **CS3-475**  
 registered-caller ring command **CS3-475**  
 req-qos command **CS3-476**  
 reset command **CS3-476**  
 resource threshold command **CS3-476**  
 response-time group command **CS3-266**  
 response-timeout command **CS3-477**  
 retry (SIP user-agent) command **CS3-478**  
 retry-delay command **CS3-477**  
 retry-limit command **CS3-478**  
 rif command **CS3-38**  
 rif timeout command **CS3-39**  
 rif validate-age command **CS3-39**  
 rif validate-enable command **CS3-39**  
 rif validate-enable-age command **CS3-40**  
 rif validate-enable-route-cache command **CS3-40**  
 ring cadence command **CS3-479**  
 ring command **CS3-478**  
 ring frequency command **CS3-480**  
 ring number command **CS3-480**  
 roaming command **CS3-480**  
 roaming (settlement) command **CS3-481**  
 rsrb remote-peer lsap-output-list command **CS3-60**  
 rsrb remote-peer netbios-output-list command **CS3-61**

rtsp client session history duration command **CS3-481**  
 rtsp client session history records command **CS3-481**  
 rule command **CS3-481**

**S**

sap-priority command **CS3-61**  
 sap-priority-list command **CS3-62**  
 sdhc address command **CS3-121**  
 sdhc dlsw command **CS3-90**  
 sdhc dte-timeout command **CS3-122**  
 sdhc frmr-disable command **CS3-122**  
 sdhc holdq command **CS3-122**  
 sdhc k command **CS3-123**  
 sdhc line-speed command **CS3-123**  
 sdhc n1 command **CS3-123**  
 sdhc n2 command **CS3-124**  
 sdhc partner command **CS3-124**  
 sdhc poll-limit-value command **CS3-125**  
 sdhc poll-pause-timer command **CS3-125**  
 sdhc poll-wait-timeout command **CS3-125**  
 sdhc qlc-prtnr command **CS3-126**  
 sdhc role command **CS3-126**  
 sdhc saps command **CS3-126**  
 sdhc sdhc-largest-frame command **CS3-127**  
 sdhc simultaneous command **CS3-127**  
 sdhc slow-poll command **CS3-127**  
 sdhc snrm-timer command **CS3-128**  
 sdhc t1 command **CS3-128**  
 sdhc test serial command **CS3-128**  
 sdhc virtual multidrop command **CS3-107**  
 sdhc vmac command **CS3-129**  
 sdhc xid command **CS3-129**  
 sdhc xid-pause-timer command **CS3-129**  
 sdllc partner command **CS3-134**  
 sdllc ring-largest-frame command **CS3-134**  
 sdllc sap command **CS3-134**  
 sdllc sdhc-largest-frame command **CS3-135**  
 sdllc traddr command **CS3-135**

- sdllc xid command **CS3-135**
- sec-profile command **CS3-266**
- security command **CS3-482**
- security (TN3270) command **CS3-266**
- send qdm message command **CS3-319**
- sequence-numbers command **CS3-483**
- server registration-port command **CS3-483**
- server trigger command **CS3-483**
- servercert command **CS3-267**
- service gprs command **CS3-585**
- service-policy command **CS3-320**
- session protocol aal2 command **CS3-485**
- session protocol command **CS3-484**
- session protocol multicast command **CS3-485**
- session protocol (VoFR) command **CS3-484**
- session target command **CS3-485**
- session target (VoIP) command **CS3-490**
- session transport command **CS3-491**
- set atm-clp command **CS3-321**
- set cos command **CS3-321**
- set ip dscp command **CS3-321**
- set ip precedence (policy-map) command **CS3-322**
- set ip precedence (route-map) command **CS3-322**
- set ip qos-group command **CS3-322, CS3-323**
- set qos-group command **CS3-323**
- settle-call command **CS3-491**
- settlement command **CS3-491**
- settlement roam-pattern command **CS3-492**
- sgcp call-agent command **CS3-492**
- sgcp command **CS3-492**
- sgcp graceful-shutdown **CS3-493**
- sgcp max-waiting-delay command **CS3-493**
- sgcp modem passthru command **CS3-493**
- sgcp quarantine-buffer disable command **CS3-494**
- sgcp request retries command **CS3-494**
- sgcp request timeout command **CS3-494**
- sgcp restart command **CS3-495**
- sgcp retransmit timer command **CS3-495**
- sgcp timer command **CS3-495**
- sgcp tse payload command **CS3-496**
- shape adaptive command **CS3-326**
- shape fecn-adapt command **CS3-326**
- shape max-buffers command **CS3-327**
- shape (policy-map class) command **CS3-325**
- show aal2 profile command **CS3-496**
- show access-expression command **CS3-40**
- show access-lists rate-limit command **CS3-327**
- show alps ascu command **CS3-167**
- show alps circuits command **CS3-168**
- show alps peers command **CS3-168**
- show atm bundle command **CS3-327**
- show atm bundle statistics command **CS3-327**
- show bridge circuit-group command **CS3-21**
- show bridge command **CS3-20**
- show bridge group command **CS3-21**
- show bridge multicast command **CS3-21**
- show bridge vlan command **CS3-22**
- show bsc command **CS3-107**
- show bstun command **CS3-107**
- show call active command **CS3-497**
- show call application voice command **CS3-497**
- show call fallback cache command **CS3-497**
- show call fallback config command **CS3-498**
- show call fallback stats command **CS3-498**
- show call history command **CS3-498**
- show call history video record command **CS3-498**
- show call history voice record command **CS3-499**
- show call resource voice stats command **CS3-499**
- show call resource voice threshold command **CS3-499**
- show call rsvp-sync conf command **CS3-499**
- show call rsvp-sync stats command **CS3-500**
- show cdapi command **CS3-500**
- show ces clock-select command **CS3-500**
- show class-map command **CS3-328**
- show connect command **CS3-500**
- show controllers channel command **CS3-232**
- show controllers rs366 command **CS3-501**
- show controllers timeslots command **CS3-501**

- show controllers token (IBM) command **CS3-41**
- show controllers voice command **CS3-502**
- show cops servers command **CS3-328**
- show csm command **CS3-502**
- show dbconn connection command **CS3-219**
- show dbconn license command **CS3-219**
- show dbconn ports command **CS3-219**
- show dbconn server command **CS3-220**
- show dbconn statistic command **CS3-220**
- show dbconn wlm command **CS3-221**
- show dhcp command **CS3-502**
- show dial-peer video command **CS3-502**
- show dial-peer voice command **CS3-503**
- show dialplan incall number command **CS3-503**
- show dialplan number command **CS3-503**
- show dlsw capabilities command **CS3-91**
- show dlsw circuits command **CS3-91**
- show dlsw fastcache command **CS3-91**
- show dlsw peers command **CS3-92**
- show dlsw reachability command **CS3-92**
- show dlsw statistics command **CS3-92**
- show dlsw transparent cache command **CS3-93**
- show dlsw transparent map command **CS3-93**
- show dlsw transparent neighbor command **CS3-93**
- show drip command **CS3-56, CS3-58**
- show dspu command **CS3-184**
- show extended channel backup command **CS3-243**
- show extended channel cmgr command **CS3-246**
- show extended channel cmpe command **CS3-246**
- show extended channel connection-map llc2  
command **CS3-232**
- show extended channel csna command **CS3-247**
- show extended channel icmp-stack command **CS3-232**
- show extended channel ip-stack command **CS3-233**
- show extended channel lan command **CS3-233**
- show extended channel llc2 command **CS3-233**
- show extended channel max-llc2-sessions  
command **CS3-234**
- show extended channel packing names command **CS3-244**
- show extended channel packing stats command **CS3-244**
- show extended channel statistics command **CS3-234**
- show extended channel subchannel command **CS3-235**
- show extended channel tcp-connections  
command **CS3-235**
- show extended channel tcp-stack command **CS3-236**
- show extended channel tg command **CS3-247, CS3-248**
- show extended channel tn3270-server client-ip-address  
command **CS3-267**
- show extended channel tn3270-server client-name  
command **CS3-268**
- show extended channel tn3270-server command **CS3-267**
- show extended channel tn3270-server dlur  
command **CS3-268**
- show extended channel tn3270-server dlurlink  
command **CS3-268**
- show extended channel tn3270-server nailed-domain  
command **CS3-268**
- show extended channel tn3270-server nailed-ip  
command **CS3-269**
- show extended channel tn3270-server nailed-name  
command **CS3-269**
- show extended channel tn3270-server pu  
command **CS3-269, CS3-272**
- show extended channel tn3270-server pu lu  
command **CS3-270**
- show extended channel tn3270-server response-time  
application command **CS3-270**
- show extended channel tn3270-server response-time  
global command **CS3-270**
- show extended channel tn3270-server response-time link  
command **CS3-271**
- show extended channel tn3270-server security  
command **CS3-272**
- show extended channel udp-listeners command **CS3-236**
- show extended channel udp-stack command **CS3-236**
- show extended max-llc2-sessions command **CS3-234**
- show frame-relay pvc command **CS3-328**
- show frame-relay vofr command **CS3-503**
- show fras command **CS3-145**
- show fras map command **CS3-146**
- show fras-host command **CS3-146**
- show gatekeeper calls command **CS3-504**

- show gatekeeper endpoints command **CS3-504**
- show gatekeeper gw-type-prefix command **CS3-504**
- show gatekeeper servers command **CS3-504**
- show gatekeeper status command **CS3-505**
- show gatekeeper zone prefix command **CS3-505**
- show gatekeeper zone status command **CS3-505**
- show gateway command **CS3-505**
- show gprs access-point command **CS3-586**
- show gprs charging parameters command **CS3-586**
- show gprs charging statistics command **CS3-586**
- show gprs gtp parameters command **CS3-586**
- show gprs gtp path command **CS3-587**
- show gprs gtp pdp-context command **CS3-587**
- show gprs gtp statistics command **CS3-587**
- show gprs gtp status command **CS3-588**
- show gprs isgsn statistics command **CS3-591**
- show interface dspfarm dsp command **CS3-505**
- show interfaces channel command **CS3-237**
- show interfaces crb command **CS3-22**
- show interfaces fair-queue command **CS3-329**
- show interfaces irb command **CS3-22**
- show interfaces random-detect command **CS3-329**
- show interfaces rate-limit command **CS3-329**
- show interfaces tokenring (IBM) command **CS3-41**
- show ip nbar protocol-discovery command **CS3-330**
- show ip rsvp atm-peak-rate-limit command **CS3-331**
- show ip rsvp command **CS3-331**
- show ip rsvp installed command **CS3-331**
- show ip rsvp interface command **CS3-332**
- show ip rsvp neighbor command **CS3-332**
- show ip rsvp policy cops command **CS3-332**
- show ip rsvp request command **CS3-333**
- show ip rsvp reservation command **CS3-333**
- show ip rsvp sbm command **CS3-333**
- show ip rsvp sender command **CS3-333**
- show l2relay statistics command **CS3-591**
- show llc2 command **CS3-130**
- show lnm bridge command **CS3-41**
- show lnm config command **CS3-41**
- show lnm interface command **CS3-42**
- show lnm ring command **CS3-42**
- show lnm station command **CS3-42**
- show local-ack command **CS3-62**
- show mgcp command **CS3-506**
- show ncia circuits command **CS3-149**
- show ncia client command **CS3-150**
- show ncia server command **CS3-150**
- show netbios-cache command **CS3-42**
- show num-exp command **CS3-506**
- show policy-map class command **CS3-334**
- show policy-map command **CS3-334**
- show policy-map interface command **CS3-334**
- show pots csm command **CS3-506**
- show pots status command **CS3-507**
- show proxy h323 calls command **CS3-507**
- show proxy h323 detail-call command **CS3-507**
- show proxy h323 status command **CS3-507**
- show qdm status command **CS3-335**
- show qlc command **CS3-136**
- show queue command **CS3-335**
- show queueing command **CS3-336**
- show queueing interface command **CS3-337**
- show rawmsg command **CS3-508**
- show rif command **CS3-43**
- show rtsp client session command **CS3-508**
- show sdhc local-ack command **CS3-136**
- show settlement command **CS3-508**
- show sgcp connection command **CS3-509**
- show sgcp endpoint command **CS3-509**
- show sgcp statistics command **CS3-509**
- show sip-ua command **CS3-510**
- show sna command **CS3-185**
- show snasw class-of-service command **CS3-193**
- show snasw connection-network command **CS3-194**
- show snasw directory command **CS3-194**
- show snasw dlctrace command **CS3-194**
- show snasw dlus command **CS3-195**
- show snasw ipstrace command **CS3-195**

- show snasw link command **CS3-196**
- show snasw lu command **CS3-196**
- show snasw mode command **CS3-197**
- show snasw node command **CS3-197**
- show snasw pdlog command **CS3-197**
- show snasw port command **CS3-197**
- show snasw pu command **CS3-198**
- show snasw rtp command **CS3-198**
- show snasw session command **CS3-199**
- show snasw statistics command **CS3-199**
- show snasw summary-ipstrace command **CS3-199**
- show snasw topology command **CS3-200**
- show source-bridge command **CS3-43**
- show span command **CS3-43**
- show spanning-tree command **CS3-22**
- show stun command **CS3-108**
- show subscriber-policy command **CS3-23**
- show tech-support rsvp command **CS3-337**
- show traffic-shape command **CS3-337**
- show traffic-shape queue command **CS3-337**
- show traffic-shape statistics command **CS3-338**
- show translation-rule command **CS3-510**
- show txconn connection command **CS3-222**
- show txconn destination command **CS3-222**
- show txconn license command **CS3-222**
- show txconn route command **CS3-222**
- show txconn server command **CS3-223**
- show txconn statistic command **CS3-223**
- show txconn transaction command **CS3-224**
- show vfc cap-list command **CS3-510**
- show vfc command **CS3-510**
- show vfc default-file command **CS3-511**
- show vfc directory command **CS3-511**
- show vfc version command **CS3-511**
- show video call summary command **CS3-511**
- show vlans command **CS3-23**
- show voice busyout command **CS3-512**
- show voice call command **CS3-512**
- show voice dsp command **CS3-513**
- show voice permanent-call command **CS3-514**
- show voice port command **CS3-514**
- show voice trunk-conditioning signaling command **CS3-517**
- show voice trunk-conditioning supervisory command **CS3-517**
- show vrm active\_calls command **CS3-517**
- show vrm vdevices command **CS3-517**
- shut command **CS3-518**
- shutdown (CMCC) command **CS3-237**
- shutdown command
  - dial-peer configuration **CS3-518**
- shutdown (DS 1 link) commands **CS3-518**
- shutdown (gatekeeper) command **CS3-519**
- shutdown (settlement) command **CS3-519**
- shutdown (TN3270) command **CS3-272**
- shutdown (voice-port) command **CS3-519**
- signal command **CS3-521**
- signal keepalive command **CS3-522**
- signal pattern command **CS3-522**
- signal sequence oos command **CS3-523**
- signal timing idle suppress-voice command **CS3-523**
- signal timing oos command **CS3-523**
- signal timing oos restart command **CS3-524**
- signal timing oos slave-standby command **CS3-524**
- signal timing oos suppress-all command **CS3-525**
- signal timing oos suppress-voice command **CS3-525**
- signal timing oos timeout command **CS3-525**
- signal-type command **CS3-526**
- sip-server command **CS3-526**
- sip-ua command **CS3-527**
- sna enable-host (QLLC) command **CS3-185**
- sna enable-host (SDLC) command **CS3-185**
- sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI) command **CS3-186**
- sna host (Frame Relay) command **CS3-186**
- sna host (QLLC) command **CS3-187**
- sna host (SDLC) command **CS3-188**
- sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC) command **CS3-189**

- sna rsrb command **CS3-189**
- sna rsrb enable-host command **CS3-190**
- sna rsrb start command **CS3-190**
- sna start command **CS3-190**
- sna vdlc command **CS3-191**
- sna vdlc enable-host command **CS3-191**
- sna vdlc start command **CS3-191**
- snasw cpname command **CS3-200**
- snasw dlcfiler command **CS3-201**
- snasw dltrace command **CS3-202**
- snasw dlus command **CS3-202**
- snasw dump command **CS3-203**
- snasw event command **CS3-204**
- snasw ip-precedence command **CS3-204**
- snasw ipsfilter command **CS3-204**
- snasw ipstrace command **CS3-205**
- snasw link command **CS3-206**
- snasw location command **CS3-207**
- snasw mode command **CS3-207**
- snasw msgdump command **CS3-208**
- snasw pathswitch command **CS3-208**
- snasw pdlog command **CS3-208**
- snasw port command **CS3-209**
- snasw start command **CS3-210**
- snasw start cp-cp command **CS3-211**
- snasw start link command **CS3-211**
- snasw start port command **CS3-211**
- snasw stop command **CS3-211**
- snasw stop cp-cp command **CS3-212**
- snasw stop link command **CS3-212**
- snasw stop port command **CS3-212**
- snasw stop session command **CS3-212**
- snmp enable peer-trap poor-qov command **CS3-527**
- source-bridge command **CS3-43**
- source-bridge connection-timeout command **CS3-44**
- source-bridge cos-enable command **CS3-62**
- source-bridge enable-80d5 command **CS3-44**
- source-bridge explorer-dup-ARE-filter command **CS3-45**
- source-bridge explorer-fastswitch command **CS3-45**
- source-bridge explorer-maxrate command **CS3-45**
- source-bridge explorerq-depth command **CS3-46**
- source-bridge fst-peername command **CS3-63**
- source-bridge input-address-list command **CS3-46**
- source-bridge input-lsap-list command **CS3-46**
- source-bridge input-type-list command **CS3-47**
- source-bridge keepalive command **CS3-63**
- source-bridge largest-frame command **CS3-63**
- source-bridge max-hops command **CS3-47**
- source-bridge max-in-hops command **CS3-47**
- source-bridge max-out-hops command **CS3-48**
- source-bridge output-address-list command **CS3-48**
- source-bridge output-lsap-list command **CS3-48**
- source-bridge output-type-list command **CS3-49**
- source-bridge passthrough command **CS3-64**
- source-bridge proxy-explorer command **CS3-49**
- source-bridge proxy-netbios-only command **CS3-49**
- source-bridge qlhc-local-ack command **CS3-136**
- source-bridge remote-peer frame-relay command **CS3-64**
- source-bridge remote-peer fst command **CS3-65**
- source-bridge remote-peer interface command **CS3-136**
- source-bridge remote-peer tcp command **CS3-65**
- source-bridge ring-group command **CS3-50**
- source-bridge route-cache cbus command **CS3-50**
- source-bridge route-cache command **CS3-50**
- source-bridge route-cache sse command **CS3-51**
- source-bridge sap-80d5 command **CS3-51**
- source-bridge sdllc-local-ack command **CS3-137**
- source-bridge spanning (automatic) command **CS3-51**
- source-bridge spanning (manual) command **CS3-52**
- source-bridge tcp-queue-max command **CS3-66**
- source-bridge transparent command **CS3-52**
- source-bridge transparent fastswitch command **CS3-53**
- source-bridge trcrf-vlan command **CS3-56, CS3-58**
- state-tracks-signal command **CS3-237**
- station name command **CS3-527**
- station number command **CS3-528**
- stun group command **CS3-108**
- stun keepalive-count command **CS3-108**

stun peer-name command **CS3-109**  
 stun protocol-group command **CS3-109**  
 stun quick-response command **CS3-109**  
 stun remote-peer-keepalive command **CS3-110**  
 stun route address interface dlci command **CS3-110**  
 stun route address interface serial command **CS3-110**  
 stun route address tcp command **CS3-111**  
 stun route all interface serial command **CS3-111**  
 stun route all tcp command **CS3-112, CS3-113**  
 stun schema offset length format command **CS3-112**  
 stun sdlc-role primary command **CS3-113**  
 stun sdlc-role secondary command **CS3-113**  
 subcell-mux command **CS3-528**  
 subscriber-policy command **CS3-23**  
 subscription-required command **CS3-588**  
 supervisory disconnect anyone command **CS3-529**  
 supervisory disconnect command **CS3-528**  
 supervisory disconnect dualtone voice-class  
 command **CS3-529**

---

**T**

tcp-port command **CS3-272**  
 tdm-group command **CS3-529**  
 tech-prefix command **CS3-530**  
 test call fallback probe command **CS3-530**  
 test pots dial command **CS3-531**  
 test pots disconnect command **CS3-531**  
 test translation-rule command **CS3-531**  
 test voice port detector command **CS3-532**  
 test voice port inject-tone command **CS3-533**  
 test voice port loopback command **CS3-535**  
 test voice port relay command **CS3-536**  
 test voice port switch command **CS3-538**  
 test vrm busyout command **CS3-539**  
 test vrm reset command **CS3-540**  
 test vrm unbusyout command **CS3-540**  
 tg (CMPC) command **CS3-248**  
 tg (CMPC+) command **CS3-248**  
 timeouts call-disconnect command **CS3-540**  
 timeouts initial command **CS3-541**  
 timeouts interdigit command **CS3-541**  
 timeouts ringing command **CS3-541**  
 timeouts wait-release command **CS3-542**  
 timers command **CS3-542**  
 timing clear-wait command **CS3-542**  
 timing delay-duration command **CS3-543**  
 timing delay-start command **CS3-543**  
 timing delay-with-integrity command **CS3-543**  
 timing dialout-delay command **CS3-544**  
 timing dial-pulse min-delay command **CS3-544**  
 timing digit command **CS3-544**  
 timing guard-out command **CS3-545**  
 timing hookflash-input command **CS3-545**  
 timing hookflash-output command **CS3-545**  
 timing interdigit command **CS3-546**  
 timing percentbreak command **CS3-546**  
 timing pulse command **CS3-546**  
 timing pulse-interdigit command **CS3-547**  
 timing wink-duration command **CS3-547**  
 timing wink-wait command **CS3-547**  
 timing-mark command **CS3-273**  
 tn3270-server command **CS3-273**  
 token-root-name command **CS3-548**  
 traffic-shape adaptive command **CS3-338**  
 traffic-shape fecn-adapt command **CS3-338**  
 traffic-shape group command **CS3-339**  
 traffic-shape rate command **CS3-339**  
 translate command **CS3-548**  
 translate-outgoing command **CS3-548**  
 translation-rule command **CS3-549**  
 transport command **CS3-549**  
 txconn destination command **CS3-225**  
 txconn license command **CS3-225**  
 txconn ping command **CS3-226**  
 txconn route command **CS3-226**  
 txconn server command **CS3-227**  
 tx-ring-limit command **CS3-340**

type command **CS3-550**  
 type (voice) command **CS3-549**

---

## U

unbind-action command **CS3-273**  
 unbundle vfc command **CS3-550**  
 unbundle vfc EXEC command **CS3-550**  
 url command **CS3-550**  
 use-interface command **CS3-588**  
 use-proxy command **CS3-551**

---

## V

vad command **CS3-552**  
 vad (dial peer) command **CS3-551**  
 vbr-rt command **CS3-552**  
 vc-hold-queue command **CS3-340**  
 vofr command **CS3-552**  
 voice call send-alert command **CS3-553**  
 voice class busyout command **CS3-554**  
 voice class codec command **CS3-554**  
 voice class dualtone command **CS3-555**  
 voice class h323 command **CS3-555**  
 voice class permanent command **CS3-556**  
 voice confirmation-tone command **CS3-557**  
 voice hunt user-busy command **CS3-558**  
 voice local-bypass command **CS3-558**  
 voice rtp send-recv command **CS3-561**  
 voice service command **CS3-561**  
 voice vad-time command **CS3-561**  
 voice-card command **CS3-554**  
 voice-class codec command **CS3-555, CS3-556**  
 voice-class permanent command **CS3-557**  
 voice-class permanent (dial-peer) command **CS3-556**  
 voice-port busyout command **CS3-560**  
 voice-port command **CS3-558**

voip-incoming translation-rule command **CS3-561**  
 vrn command **CS3-274**

---

## X

x25 map bridge command **CS3-24**  
 x25 map qllc command **CS3-137**  
 x25 pvc qllc command **CS3-139**

---

## Z

zone access command **CS3-562**  
 zone bw command **CS3-562**  
 zone local command **CS3-563**  
 zone prefix command **CS3-563**  
 zone remote command **CS3-564**  
 zone subnet command **CS3-565**

